



Written by Daniel J. Solove

[www.teachprivacy.com](http://www.teachprivacy.com)

Illustrated by Ryan Beckwith

**Рассмотрение механизмов и специфики применения | Алексей Мунтян**  
**Общего регламента ЕС по защите данных (GDPR) | 31.03.2024**

**Disclaimer:** данная работа является систематизированным собранием (компиляцией) как материалов, созданных самим автором, так подготовленных и (или) опубликованных в открытых источниках иными лицами.

## 2 Содержание

1. [Обзор контекста принятия и механизмов GDPR](#)
2. [Персональные данные, принципы обработки и права субъектов](#)
3. [Accountability и демонстрация соответствия](#)
4. [Records of processing activities и сроки хранения данных](#)
5. [Прозрачность обработки данных и повышение осведомленности](#)
6. [Processing grounds and Legitimate Interests Assessment](#)
7. [Data Protection \(Privacy\) by Design and by Default](#)
8. [Data Protection Impact Assessment](#)
9. [Data Breach Management](#)
10. [Data Protection Officer](#)
11. [Роли в обработке персональных данных](#)
12. [Соглашения об обработке и защите персональных данных](#)
13. [Интернет-ресурсы, профилирование и прямой маркетинг \(реклама\)](#)
14. [Обработка данных персонала и соискателей](#)
15. [Биометрические данные и видеонаблюдение](#)
16. [Обработка данных несовершеннолетних лиц](#)
17. [Большие данные, искусственный интеллект, машинное обучение и блокчейн](#)
18. [Автоматизация Privacy и Data Protection](#)
19. [Технические и организационные меры защиты персональных данных](#)
20. [Псевдонимизация и анонимизация](#)
21. [Территориальная сфера действия GDPR](#)
22. [Трансграничная обработка данных и Transfer Impact Assessment](#)
23. [EU-US Data Privacy Framework](#)
24. [Рекомендации, руководства и практические пособия](#)
25. [Международные стандарты](#)
26. [Правоприменительная практика](#)
27. [Штрафы – базы дел и аналитика](#)
28. [Штрафы – интересные кейсы](#)
29. [Иные санкции и меры принуждения](#)
30. [Судебная практика – базы решений и интересные ситуации](#)
31. [Влияние GDPR на бизнес](#)
32. [Итоги применения GDPR в 2018-2023гг. и дальнейшие перспективы](#)
33. [Законодательные инициативы о персональных данных в ЕС и США](#)
34. [Эра пост-GDPR в Великобритании](#)
35. [Подборка ресурсов по GDPR](#)
36. [Модернизация Конвенции 108 и влияние GDPR на РФ](#)

## Обзор контекста принятия и механизмов GDPR



# 4 Эволюция европейского законодательства о защите данных (I)

2016 (EU)  
EU-US PrivacyShield approved

2013 (OECD)  
OECD Guidelines updated

2018 (CoE)  
Convention 108 updated

2016 (EU)  
NIS Directive

2016 (EU)  
Law Enforcement Directive

2016 (EU)  
PNR Directive

20?? (EU)  
ePrivacy Regulation

2016 (EU)  
GDPR

2008 (EU)  
Council Framework Decision (data in law enforcement situations)

2009 (EU)  
ePrivacy Directive amended

2006 (EU)  
Data Retention Directive (later repealed)

2000 (EU)  
Safe Harbour decision (later overturned)

2001 (CoE)  
Convention 108 amended

2002 (EU)  
ePrivacy Directive

2000 (EU)  
E-Commerce Directive

1995 (EU)  
Data Protection Directive

1981 (CoE)  
Convention 108

1980 (OECD)  
OECD Guidelines

1979  
Data protection laws enacted in 7 member states

1973/4 (CoE)  
Resolutions 73/22 (private sect.) & 74/29 (publicsec.)

1973  
First national privacy law: Data Act, Sweden

1970  
First modern privacy law. Hesse, Germany

1950 (CoE)  
The European Convention on Human Rights (ECHR)

1948 (UN)  
The Universal Declaration of Human Rights



UN founded

Relevant context and data protection law

1951  
Treaty of Paris - ECSC created

1957  
Treaty of Rome - EEC created

1958  
Euratom created

1965  
Merger Treaty

1986  
Single European Act (SEA) amended

1992  
Maastricht Treaty

2000  
Charter of Fundamental Rights of the EU

2007  
Treaty of Lisbon

European structural evolution

1950 1960 1970 1980 1990 2000 2010 2018

Evolution of technology



Society

WW2 atrocities

Shared European coal & steel production

Growth of international trade

Increasing use of IT & telecommunications

Direct marketing

Telemarketing

Data mining

Identity thefts

9/11

High profile data breaches and/or concerns

2004 Madrid bombings

2005 London bombings

Edward Snowden disclosures about global surveillance

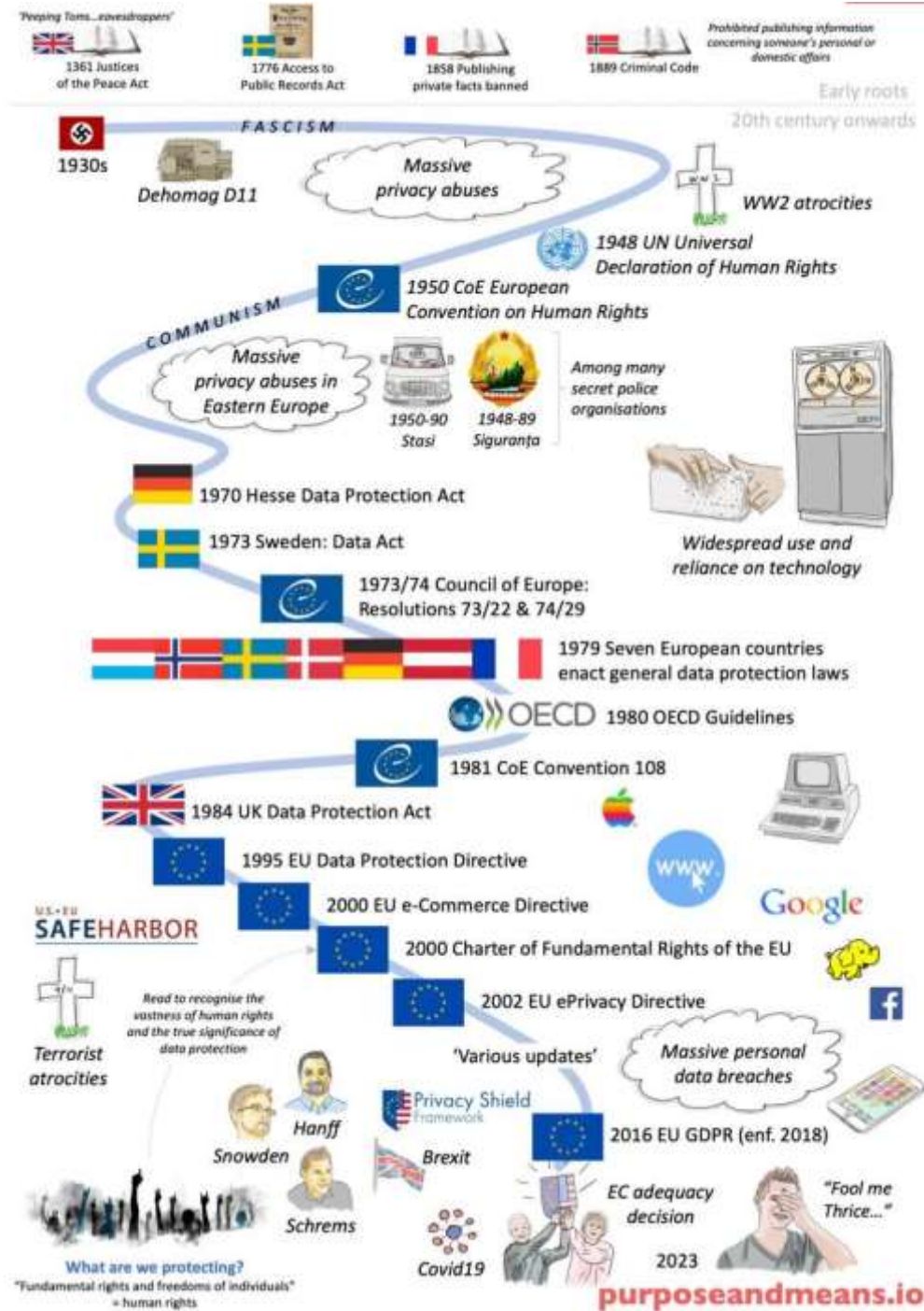
Max Schrems

#metoo

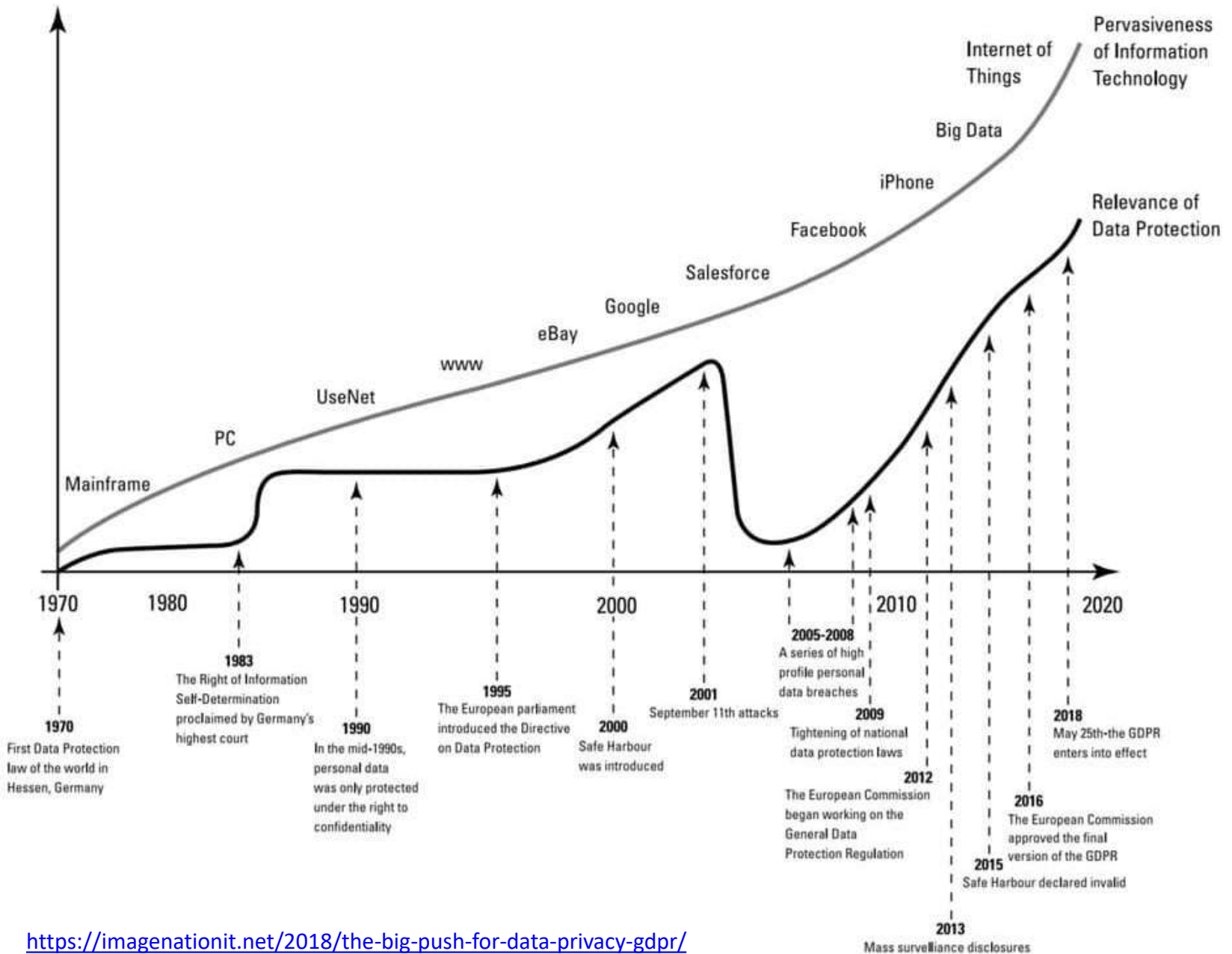
Social Media Trends

<https://www.linkedin.com/in/tim-clements-fbcs-citp-cippe-cipm-cipt-638651/>

# Эволюция европейского законодательства о защите данных (II)



## 6 Эволюция восприятия защиты персональных данных



## 7 Что такое GDPR?

[Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**) – это новый регламент ЕС о защите персональных данных, формирующий обязательные к соблюдению единые принципы и подходы как для государств-членов ЕС, так и для некоторых иных государств (Исландия, Лихтенштейн, Норвегия). 19.04.2018 проведена [гармонизация](#) прочтения некоторых положений GDPR на разных языках ЕС.

### Некоторые факты:

- вступил в силу 25.05.2018
- заменяет собой Директиву 95/46/ЕС от 24.10.1995
- гармонизирует правотворчество и правоприменение
- действует не только в ЕС, но и в иных странах, которые осуществили имплементацию норм GDPR – [Норвегии](#), [Лихтенштейне](#), [Исландии](#) в рамках [Европейской ассоциации свободной торговли](#) (за исключением Швейцарии)
- локальный надзор осуществляется национальными органами стран-участниц Евросоюза по защите данных (Data Protection Authorities)
- общий надзор осуществляется Европейским советом по защите данных (European Data Protection Board)
- непосредственно применяется национальными судами государств-членов ЕС и Судом справедливости Евросоюза (European Court of Justice)

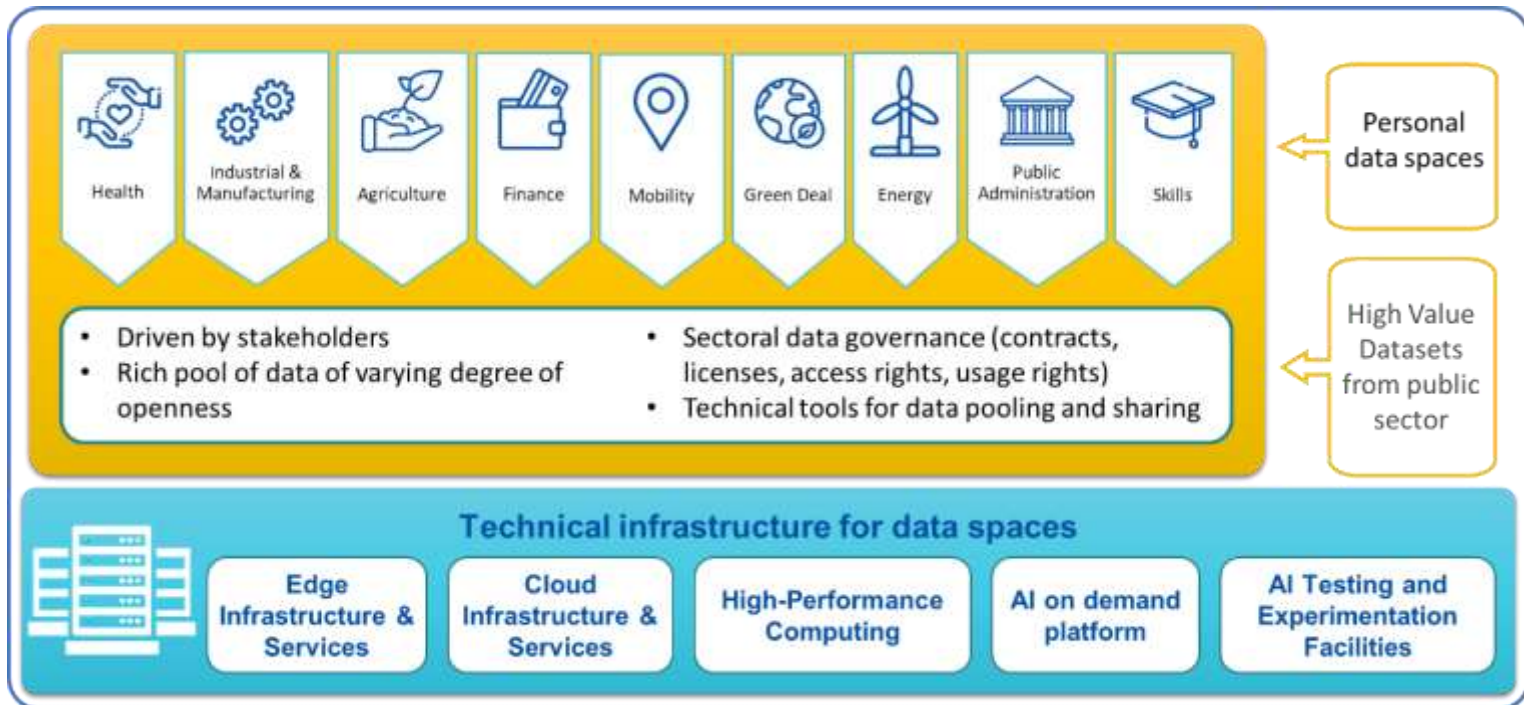
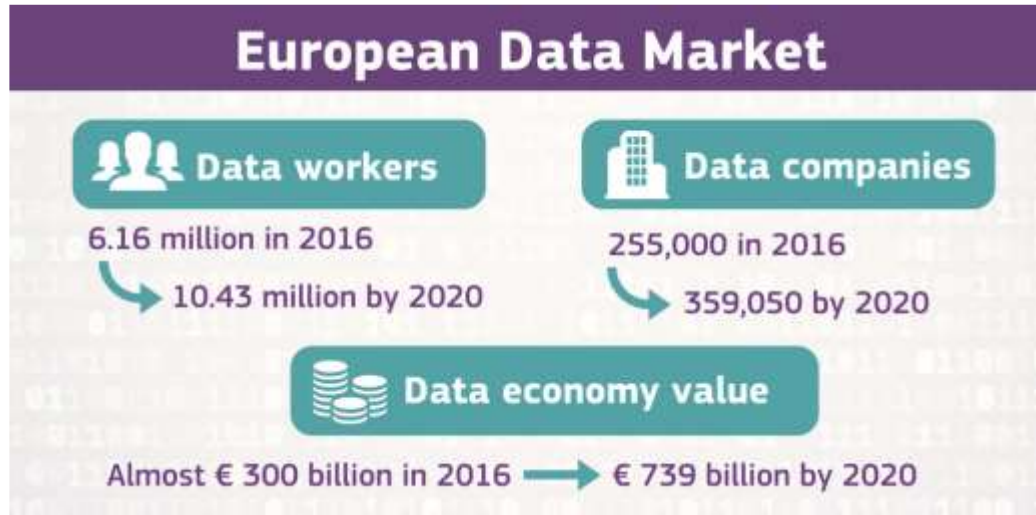
### Полезные ссылки:

- [общее описание реформы правил по защите данных в ЕС](#);
- [национальные органы стран-участниц ЕС по защите данных](#);
- [иконографика по GDPR от Европейской Комиссии](#);
- [Directive 2002/58/EC](#) of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

## 8 GDPR как часть Digital Single Market Strategy

- Идеи об усилении безопасности в цифровой сфере Еврокомиссия обобщила в [Сообщении](#) от 28.04.2015 «Европейская повестка дня в сфере безопасности» (The European Agenda on Security).
- Европейская Комиссия 06.05.2015 анонсировала масштабную программу [Digital Single Market](#), призванную улучшить работу единого европейского рынка, и особенно его цифрового сегмента. Задачи поставлены грандиозные – расцвет экономики данных и онлайн-бизнес-проектов, доступность контента пользователям, защищенность интересов авторов.
- 10.01.2017 Еврокомиссия опубликовала [Сообщение](#) «Обмен и охрана персональных данных в глобализованном мире» (Communication Exchanging and Protecting Personal Data in a Globalised World), которое посвящено трансграничной передаче данных и международным инструментам охраны.
- 19.02.2020 Европейская комиссия опубликовала сообщение [A European strategy for data](#). В документе представлен подход, как с использованием законодательных и общественных инициатив, технических стандартов ЕС станет дата-лидером и создаст более либеральную экономику данных. В этот же день было опубликовано другое важное сообщение ЕК [Shaping Europe's Digital Future](#).





## 10 GDPR как часть реформы европейского права

[Regulation \(EU\) 910/2014](#) of 23.07.2014 (**electronic IDentification, Authentication and trust Services Directive – eIDAS**) on electronic identification and trust services for electronic transactions in the internal market

[Directive \(EU\) 2016/680](#) of 27.04.2016 (**Law Enforcement Directive – LED** или **Police Data Protection Directive - PDPD**) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

[Directive \(EU\) 2016/943](#) of 08.06.2016 (**Trade Secrets Directive – TSD**) on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

[Regulation \(EU\) 2018/1725](#) of 23.10.2018 (**Data Protection Regulation for the EU Institutions – DPEUI**) on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data

[Regulation \(EU\) 2018/1807](#) of 14.11.2018 (**Free Flow Data – FFD**) on a framework for the free flow of non-personal data in the EU

[Regulation \(EU\) 2019/881](#) of 17.04.2019 (**Cybersecurity Act – CSA**) on ENISA and on information and communications technology cybersecurity certification

[Directive \(EU\) 2019/770](#) of 20.05.2019 (**Digital Content Directive – DCD**) on certain aspects concerning contracts for the supply of digital content and digital services

[Directive \(EU\) 2019/1024](#) of 20.06.2019 (**Open Data Directive – ODD**) on open data and the re-use of public sector information

[Regulation \(EU\) 2019/1150](#) of 20.06.2019 on promoting fairness and transparency for business users of online intermediation services (см. ст.9) + [Guidelines on ranking transparency](#)

[Directive \(EU\) 2020/1828](#) of 25.11.2020 on representative actions for the protection of the collective interests of consumers

[Regulation \(EU\) 2022/868](#) of 30.05.2022 (**Data Governance Act – DGA**) on European Data Governance

[Regulation \(EU\) 2022/1925](#) of 14.09.2022 (**Digital Markets Act – DMA**) on contestable and fair markets in the digital sector

[Regulation \(EU\) 2022/2065](#) of 19.10.2022 (**Digital Services Act – DSA**) on a Single Market For Digital Services

[Directive \(EU\) 2022/2555](#) of 14.12.2022 (**Networking and Information Security 2 Directive – NIS 2 Directive**) concerning measures for a high common level of security of network and information systems across the Union

[Proposal for a Regulation](#) laying down harmonised rules on artificial intelligence (**Artificial Intelligence Act – AIA**)

[Proposal for a Regulation](#) on digital products and ancillary services (**Cyber Resilience Act – CRA**)

[Proposal for a Directive](#) on adapting non contractual civil liability rules to artificial intelligence

[Proposal for a Regulation](#) on harmonised rules on fair access to and use of data (**Data Act**)

[Proposal for a Regulation](#) on laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679

## Тексты (на английском языке) основных правовых privacy-актов в ЕС/ЕАСТ и Великобритании

- [The Federal Data Protection Act \(Germany\)](#)
- [The Data Protection Law n°2018-493 \(France\)](#)
- [Personal Data Protection Code - legislative decree No. 196/2003 \(Italy\)](#)
- [The Organic Law on Data Protection and Digital Rights Guarantee \(Spain\)](#) (включая право отключить рабочий телефон и не проверять рабочую почту в нерабочее время, свобода от видеонаблюдения на рабочем месте)
- [The Data Protection Act \(Ireland\)](#)
- [The Data Protection Act 2018 \(United Kingdom\)](#)

## 12 Digital Services Act, регулирующий обработку данных для онлайн-рекламы

Закон о цифровых услугах (Digital Services Act - DSA) дополняет Закон о цифровых рынках (Digital Markets Act - DMA), который направлен на регулирование крупных технологических компаний. Оба акта вступили в силу в 2023г.

**DSA затрагивает ИТ-платформы и онлайн-посредников**, включая социальные сети, магазины приложений как AppStore и Google Play, стриминговые платформы и другие цифровые торговые площадки.

Закон применяется к компаниям, базирующимся за пределами ЕС, но оказывающим услуги на едином рынке ЕС: им придется назначить законного представителя в ЕС (но аналогичное обязательство уже накладывалось на них ранее в GDPR – европейском законе о персональных данных). Любая компания, нарушившая DSA, может быть **оштрафована на сумму до шести процентов от ее глобального дохода**.

**DSA предполагает:**

- запрет использовать «чувствительные» персональные данные, включая информацию о расе, религии и сексуальной ориентации, в таргетированной рекламе;
- запрет на таргетированную рекламу для несовершеннолетних лиц;
- запрет на так называемые «dark patterns» («непрозрачные схемы») – пользовательские интерфейсы, вынуждающие пользователей делать то, чего они делать не собирались (в тексте акта это сформулировано как «запрещено обманывать или подталкивать получателей услуги, а также искажать или ограничивать автономию принятия решений или выбор получателей услуги через структуру, дизайн или функциональные возможности онлайн-интерфейса или его часть»);
- обязанность давать пользователям возможность принимать решения в отношении рекламы, которую они видят (они должны быть четко проинформированы о том, как и почему ему было показано конкретное рекламное объявление и кто заплатил за рекламу; крупные онлайн-платформы (более 45 млн пользователей) должны будут хранить и предоставлять доступ к репозиториям объявлений, позволяя исследователям и властям проверять, как организован показ рекламных сообщений, манипулируют ли их рекламные системы и каким образом);
- обязанность предоставить пользователям возможность легко отказаться от использования их данных в рекламных целях;
- обязанность платформ удалять незаконный контент и предотвращать распространение дезинформации (пользователи смогут пометать незаконный контент, и платформа будет обязана уведомлять их о своих решениях);
- гарантию, что потребители могут покупать безопасные товары в Интернете, усиливая обязательство площадок проверять продавцов (принцип «Знай своего бизнес-клиента»).

Комиссия ЕС 20.10.2023 утвердила [правила](#) проведения независимых аудитов в рамках DSA.


## 13 Data Act, регулирующий обработку данных от подключённых устройств

Законопроект предусматривает, в частности:

1. Меры, которые обеспечат пользователям подключённых устройств доступ к данным, сгенерированным этими устройствами и сервисами, имеющими отношение к подобным устройствам. Пользователи смогут делиться этими данными со сторонними лицами или организациями, что поспособствует развитию услуг в области послепродажного обслуживания и инноваций. Предполагается, что производители устройств останутся заинтересованы в инвестициях в генерацию высококачественных данных с учётом того, что их ноу-хау останутся под охраной.
2. Меры, обеспечивающие защиту от несправедливых условий договоров, которые выдвигаются в одностороннем порядке. Цель — защита европейских компаний от нечестных соглашений, стимулирование честных переговоров, обеспечение более уверенного присутствия малого и среднего бизнеса на электронных торговых площадках.
3. Механизмы для государственных организаций, позволяющие получать доступ и использовать данные, хранящиеся частными компаниями, в случае введения чрезвычайного положения, например, из-за наводнений или лесных пожаров или при исполнении юридического требования, когда необходимые данные невозможно получить по первому требованию другими способами. Документ предусматривает новые правила, обеспечивающие гражданам свободу менять различных поставщиков услуг облачной обработки данных. Эти правила призваны продвигать конкуренцию и свободу выбора на рынке и одновременно противодействовать ситуации, когда потребители попадают в зависимость от компании-поставщика. Кроме того, Data Act предусматривает защитные механизмы, направленные против [незаконной передачи](#) данных и обеспечивающие более надёжные и безопасные условия для обработки данных.
4. Меры, способствующие развитию стандартов совместимости в области передачи и обработки данных в координации с соответствующей стратегией ЕС.

Европарламент [одобрил](#) закон о защите данных, который отправлен на дальнейшее одобрение Совету ЕС.

## 14 Networking and Information Security Directive 2.0

 Council of the European Union

Brussels, 26 November 2021  
(OR. en)

14337/21

Interinstitutional File:  
2020/0359(COD)

CODEC 1541  
CSC 416  
CSCI 147  
CYBER 312  
DATAPROTECT 269  
JAI 1295  
MI 891  
TELECOM 436

**NOTE**

From: General Secretariat of the Council  
To: Council

No. prev. doc.: 9583/2/21, 11724/21  
No. Cion doc.: 14150/20

Subject: Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148  
- General Approach

**I. INTRODUCTION**

1. On 16 December 2020, the Commission adopted the proposal for a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or "NIS 2")<sup>1</sup> with the aim to replace the current Directive on security of network and information systems ("the NIS Directive")<sup>2</sup>.

<sup>1</sup> Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

<sup>2</sup> Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

14337/21 EB/es I  
JAI.2 EN

Европарламент принял проект обновленной Директивы о безопасности сетей и информационных систем в ЕС (NIS2 Directive).

Директива установит базовый перечень для мер по управлению рисками кибербезопасности и обязательств по предоставлению отчетности в критически важных секторах (например, энергетика, транспорт, здравоохранение и цифровая инфраструктура).

NIS2 направлен на устранение расхождений в требованиях к кибербезопасности и в реализации мер кибербезопасности в разных государствах-членах ЕС.

Кроме того, была проведена работа по более четкому определению правил взаимодействия между нормами NIS2 и отраслевого законодательства – Законом о цифровой операционной устойчивости (DORA) и Директивой об устойчивости критически важных объектов (CER).

## Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence



Brussels, 28.9.2022  
COM(2022) 496 final  
2022/0303 (COD)

Proposal for a

**DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on adapting non-contractual civil liability rules to artificial intelligence  
(AI Liability Directive)**

(Text with EEA relevance)

{SEC(2022) 344 final} - {SWD(2022) 318 final} - {SWD(2022) 319 final} -  
{SWD(2022) 320 final}

◇ Еврокомиссия 28.09.2022 предложила принять новые нормы, которые сделают судебное преследование производителей небезопасных ИИ-продуктов проще для граждан и организаций ЕС.

◇ Инициатива выдвинута с учётом постоянно растущего количества ИИ-продуктов в Евросоюзе — дронов, роботов и подобной техники.

◇ Согласно предложенным Еврокомиссией правилам, пострадавшие смогут требовать компенсацию за нанесённый ущерб жизни, собственности, здоровью, за нарушение прав на неприкосновенность личной жизни из-за недостатков товара или ошибки провайдера, разработчика или пользователя ИИ-технологии, а также за дискриминацию при устройстве на работу.

◇ Правила облегчают бремя доказывания для жертв при помощи «презюмции причинности» (presumption of causality). От пострадавших потребуется только продемонстрировать, что неспособность производителя или пользователя выполнить определённые требования причинила ущерб, и затем увязать этот факт с ИИ-технологиями в иске.

◇ Пострадавшие могут попросить суд затребовать от компаний и поставщиков информацию о ИИ-системах с высоким уровнем опасности, чтобы установить виновного и неисправность, повлекшую ущерб.

## 16 Proposal for a regulation on the transparency and targeting of political advertising

Председательствующая в Совете ЕС Испания и представители Европарламента предварительно договорились об основных деталях нового закона, касающегося прозрачности и таргетирования политической рекламы.

Декларируемая цель — облегчить идентификацию политической рекламы для граждан ЕС, которые смогут понять, кто стоит за подобной рекламой, и сделать осознанный выбор.

Документ определяет политическую рекламу как подготовку, размещение, продвижение, публикацию, доставку и распространение сообщений:

- ◇ от политических деятелей, для них или в их интересах, если такие сообщения не носят исключительно частный или коммерческий характер;
- ◇ могут быть или специально предназначены для оказания влияния на поведение электората, на результаты выборов, референдумов или законодательного процесса на всех уровнях в ЕС.

Согласно документу, использование персональных данных для таргетированной политической рекламы будет разрешено только в том случае, если данные были получены от субъекта данных, который дал явное согласие на использование подобной информации для политической рекламы.

Подразумевается введение полного запрета на таргетированную политическую рекламу с использованием отдельных категорий персональных данных, раскрывающих этническое и расовое происхождение или политические убеждения европейцев.

Для недопущения внешнего вмешательства законодатели договорились о запрете предоставления рекламных услуг спонсорам из третьих стран за три месяца до проведения выборов или референдумов.

<https://www.consilium.europa.eu/media/60812/st16013-re01-en22.pdf>

<https://www.consilium.europa.eu/en/press/press-releases/2023/11/07/transparency-and-targeting-of-political-advertising-eu-co-legislators-strike-deal-on-new-regulation/>



## 17 Европейская декларация о цифровых правах и принципах



Председатели Европейской комиссии, Европейского парламента и Европейского совета 15.12.2022 подписали Европейскую декларацию о цифровых правах и принципах ("Декларация"), предложенную Комиссией в январе 2022 года и направленную на поддержку целей Цифрового компаса 2030 года. Декларация представляет собой обязательство ЕС по безопасной, надежной и устойчивой цифровой трансформации, которая ставит права человека во главу угла, ориентирует политиков и компании, работающие с новыми технологиями, и намерена направлять подход ЕС к цифровой трансформации в глобальном масштабе. Декларация предусматривает:

- ◇ неприкосновенность частной жизни и индивидуальный контроль над данными, отмечая, что каждый человек имеет право на неприкосновенность частной жизни и на защиту своих персональных данных, причем последнее включает контроль со стороны человека над тем, как используются его персональные данные и с кем они передаются;
- ◇ право каждого человека на конфиденциальность своих сообщений и информации на своих электронных устройствах и не подвергаться незаконному наблюдению в Интернете, незаконному повсеместному отслеживанию или мерам по перехвату;
- ◇ возможность для каждого человека определять свое цифровое наследие и решать, что произойдет с его личными счетами и информацией, которая его касается, после его смерти.

## 18 Европарламент одобрил закон об искусственном интеллекте (AI Act)

◇ Депутаты Европарламента 11.03.2024 одобрили закон (Artificial Intelligence Act) об искусственном интеллекте (ИИ).

◇ Закон запрещает «интрузивное и дискриминационное использование ИИ-систем», в частности:

- систем дистанционной биометрической идентификации, работающих в режиме реального времени в общедоступных местах;
- систем дистанционной биометрической идентификации, используемых постфактум, за исключением их применения правоохранными органами с санкции суда для расследования тяжких преступлений;
- биометрических классификационных систем, использующих «деликатные характеристики» (пол, расу, этническую и религиозную принадлежность, гражданство, политические пристрастия).
- прогностических систем полиции (работа которых основана на фактах биографии, местоположении или преступных деяниях, совершённых [физическим лицом] в прошлом);
- систем распознавания эмоций правоохранными органами, пограничным контролем, работодателями и образовательными организациями.

◇ Запрещён также неизбирательный сбор биометрических данных из соцсетей или записей с камер наблюдения для создания баз данных, используемых в системах распознавания лиц (с нарушением прав человека и права на неприкосновенность частной жизни).

◇ Классификация сфер высокого риска включает ущерб здоровью, безопасности, фундаментальным правам человека и вред окружающей среде. В список ИИ-инструментов, связанных с высоким риском, внесены ИИ-системы, которые оказывают влияние на избирателей во время проведения политических кампаний, и рекомендательные алгоритмы интернет-платформ (с ежемесячной аудиторией более 45 миллионов человек по закону о цифровых услугах — Digital Services Act, DSA).

◇ Поставщики базовых ИИ-моделей обязаны давать гарантии полноценного обеспечения фундаментальных прав, верховенства закона, безопасности, а также защиты здоровья, окружающей среды и демократии. Поставщикам придётся оценивать и минимизировать риски, учитывать требования по разработке и охране окружающей среды, регистрироваться в специальной базе данных ЕС.

◇ Создатели генеративных базовых моделей, таких как ChatGPT, будут должны выполнять дополнительные требования для обеспечения прозрачности — указывать факт создания контента при помощи ИИ, разрабатывать модель таким образом, чтобы не допустить генерацию незаконного контента, а также публиковать сведения о защищённых авторскими правами данных, использованных при обучении ИИ-систем.

◇ Для граждан предусматривается возможность подавать жалобы на работу ИИ-систем и получать разъяснения относительно решений, принятых на основе [рекомендаций] ИИ-систем и влияющих на права жителей ЕС.

## 19 Новая редакция законопроекта об искусственном интеллекте (AI Act)

В "Закон о ИИ" войдут многие положения по весьма жёсткому регулированию создания, применения и эксплуатации ИИ.

В частности будет запрещена эксплуатация ИИ следующих категорий:

- системы биометрической категоризации, использующие чувствительные характеристики (например, политические, религиозные, философские убеждения, сексуальная ориентация, раса);
- нецелевое извлечение изображений лиц из Интернета или записей с камер видеонаблюдения для создания баз данных для распознавания лиц;
- распознавание эмоций на рабочем месте и в учебных заведениях;
- социальный рейтинг, основанный на социальном поведении или личных характеристиках;
- системы искусственного интеллекта, которые манипулируют поведением людей, чтобы обойти их свободную волю;
- ИИ используемый для эксплуатации уязвимостей людей (из-за их возраста, инвалидности, социального или экономического положения).


За исключением таких задач как:

- целевые поиски жертв (похищение, торговля людьми, сексуальная эксплуатация),
- предотвращение конкретной и существующей террористической угрозы или
- локализация или идентификация лица, подозреваемого в совершении одного из конкретных преступлений

А также будут установлены требования к прозрачности ИИ продуктов и создание "песочниц" по контролю национальных властей для разработки ИИ малым и средним бизнесом без влияния глобальных корпораций.

Штрафы за нарушение могут достигать 7% от глобального оборота компании, так что последствия нарушений будут серьёзными, для многих компаний на кону может стоять принципиальное решение присутствовать или нет на рынке ЕС. Многие будут зависеть от того когда те или иные требования закона будут запланированы к исполнению.

European Commission - Press release



### DSA enforcement: Commission launches European Centre for Algorithmic Transparency

Brussels, 17 April 2023

Tomorrow, the [European Centre for Algorithmic Transparency \(ECAT\)](#) will be officially inaugurated by the Commission's [Joint Research Centre](#) in Seville, Spain. The inauguration will be marked with a launch event that will be broadcast [here](#).

The event brings together representatives from EU institutions, academia, civil society and industry to discuss the main challenges and the importance at a societal level of having oversight of how algorithmic systems are used. Following a video message by Commissioner for the Internal Market Thierry **Bretton**, the audience will dive into the current and planned work of ECAT, including a preliminary showcase of its potential through live demos.

#### The role of ECAT under the Digital Services Act

The [Digital Services Act](#) imposes risk management requirements for companies designated by the European Commission as Very Large Online Platforms and Very Large Online Search Engines. Under this framework, designated platforms will have to identify, analyse and mitigate a wide array of systemic risks on their platforms, ranging from how illegal content and disinformation can be amplified through their services, to the impact on the freedom of expression or media freedom. Similarly, specific risks around gender-based violence online and the protection of minors online and their mental health must be assessed and mitigated. The risk mitigation plans of designated platforms' and search engines will be subject to an independent audit and oversight by the European Commission.

ECAT will provide the Commission with in-house technical and scientific expertise to ensure that algorithmic systems used by the Very Large Online Platforms and Very Large Online Search Engines comply with the risk management, mitigation and transparency requirements in the DSA. This includes, amongst other tasks, the performance of **technical analyses and evaluations of algorithms**. An interdisciplinary team of data scientists, AI experts, social scientists and legal experts will combine their expertise to assess their functioning and propose best practices to mitigate their impact. This will be crucial to ensure the thorough analysis of the transparency reports and risk self-assessment submitted by the designated companies, and to carry out inspections to their systems whenever required by the Commission.

This mission could not be attained without proper **research and foresight capacity**, which are also inherent to ECAT's approach. JRC researchers will build on and further advance their longstanding expertise in the field of Artificial Intelligence (AI), which has already been instrumental in the preparation of other milestone pieces of regulation like the [AI Act](#), the [Coordinated Plan on AI](#) and its 2021 review. ECAT researchers will not only focus on identifying and addressing systemic risks stemming from Very Large Online Platforms and Very Large Online Search Engines, but also investigate the long-term societal impact of algorithms.

#### Background

On 15 December 2020, the Commission made the [proposal](#) on the DSA together with the proposal on the Digital Markets Act (DMA) as a comprehensive framework to ensure a safer, more fair digital space for all. Following the [political agreement](#) reached by the EU co-legislators in April 2022, the DSA [entered into force](#) on 16 November 2022. The deadline for platforms and search engines to publish the number of their monthly active users was on 17 February 2023. The Commission is now in process of analysing the publications with a view to designating Very Large Online Platforms and Very Large Online Search Engines, which will have four months from the designation to comply with all DSA obligations and in particular to submit their first risk assessment. By 17 February 2024 the DSA will apply to all intermediary services; by the same date Member States are required to appoint Digital Services Coordinators.

The DSA applies to all digital services that connect consumers to goods, services, or content. It

Европейская комиссия объявила о начале работы 18.04.2023 Европейского центра алгоритмической прозрачности ("ECAT"), который будет предоставлять Комиссии собственные технические и научные знания для обеспечения того, чтобы алгоритмические системы, используемые "Очень крупными онлайн-платформами" и "Очень крупными онлайн-поисковыми системами" в соответствии с Регламентом (ЕС) 2022/2065 (Закон о цифровых услугах, "DSA"), соответствовали установленным в нем требованиям по управлению рисками, их снижению и прозрачности. ECAT будет осуществлять проведение технического анализа и оценки алгоритмов.



**PRIVAZYPLAN®**  
GETS YOUR DATA PROTECTION  
ON COURSE.

The EU general data protection regulation 2016/679 (GDPR) will take effect on 25 May 2018. Unfortunately, Brussels has not provided a clear overview of the 99 articles and 173 recitals. The [PrivacyPlan®](#) fills this gap (with a table of contents, cross-references, emphases, corrections and a dossier function). Data protection/Privacy/Privazy according to plan.

# EU General Data Protection Regulation (EU-GDPR) Table of contents

[Info](#) / [Regulation](#) / [Dossier](#)

4.5.2016 | EN | Official Journal of the European Union | L 119/1 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [...]

## CHAPTER I - General provisions

[Article 1](#) - Subject-matter and objectives (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13)

[Article 2](#) - Material scope (14, 15, 16, 17, 18, 19, 20, 21)

[Article 3](#) - Territorial scope (22, 23, 24, 25)

[Article 4](#) - Definitions (26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37)

## CHAPTER II - Principles

[Article 5](#) - Principles relating to processing of personal data (39)

[Article 6](#) - Lawfulness of processing (40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 155)

[Article 7](#) - Conditions for consent (32, 33, 42, 43)

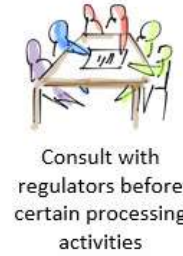
[Article 8](#) - Conditions applicable to child's consent in relation to information society services (38)

[Article 9](#) - Processing of special categories of personal data (51, 52, 53, 54, 55, 56)

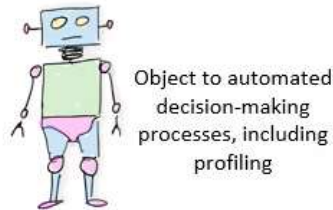
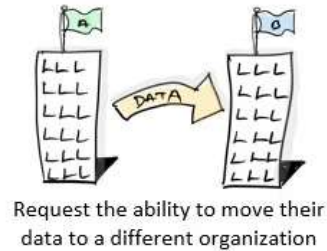
[Article 10](#) - Processing of personal data relating to criminal convictions and offences

[Article 11](#) - Processing which does not require identification (57, 64)

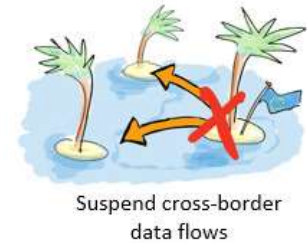
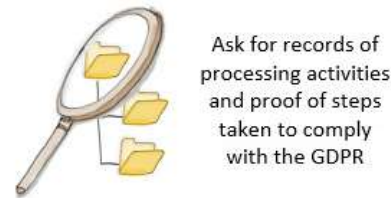
## What organizations have to do



## What individuals can do



## What regulators can do



# 23 GDPR на одной странице от TeachPrivacy

## TERRITORIAL SCOPE



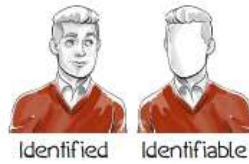
EU Establishments

Non-EU Established Organizations  
Offer goods or services or engaging in monitoring within the EU.

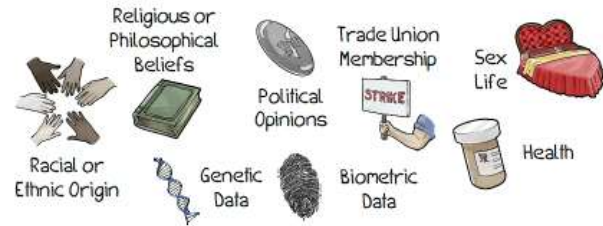
## THE PLAYERS



## PERSONAL DATA



## SENSITIVE DATA



## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS



## LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



## CONSENT

Consent must be freely given, specific, informed, and unambiguous.

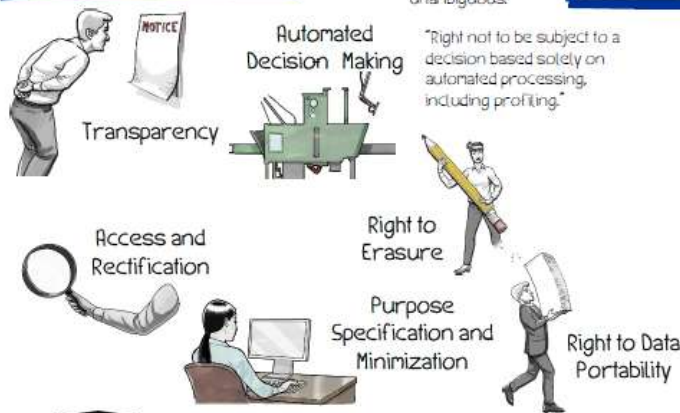


## DATA BREACH NOTIFICATION

A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects  
Notify supervisory authorities no later than 72 hours after discovery.

## RIGHTS OF DATA SUBJECTS

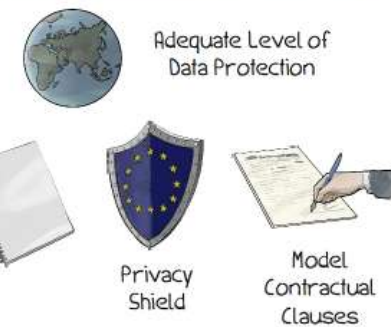


## ENFORCEMENT

Fines  
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies: compensation for material and non-material harm.

## INTERNATIONAL DATA TRANSFER



## 24 Механизмы GDPR, на которые стоит обратить особое внимание

- Legitimate Interests Assessment (Art.6) – Оценка сбалансированности законных интересов субъекта и контролера
- Privacy Notices (Art.12-14) - Предоставляемая информация при сборе персональных данных
- Right To Be Forgotten (Art.17) - Право на удаление данных («право на забвение»)
- Right To Data Portability (Art.20) - Право на переносимость данных
- Automated individual decision-making, including profiling (Art.22) - Автоматизированное индивидуальное принятие решений, включая составление профиля
- Data Protection By Default (Art.25) - Защита данных по умолчанию
- Data Protection By Design (Art.25, 32) – Проектируемая защита данных
- Representatives of Non-EU Controllers or Processors (Art.27) - Представители контролеров или обработчиков, не учрежденных в Евросоюзе
- Personal Data Breach Notification (Art.33) - Уведомление надзорного органа об утечке персональных данных
- Personal Data Breach Communication (Art.34) - Сообщение субъекту данных об утечке персональных данных
- Data Protection Impact Assessment<sup>1</sup> (Art.35) - Оценка воздействия на защиту данных
- Prior Consultation (Art.36) - Предварительная консультация
- Data Protection Officer (Art.37-39) - Назначение на должность инспектора по защите персональных данных
- Data Protection Certification (Art.42) - Сертификация
- One-Stop-Shop Supervisory Mechanism (Rec.127-128) - Сотрудничество между руководящим надзорным органом и заинтересованными надзорными органами («механизм единого окна»)

<sup>1</sup> См. заключение EDPB - [https://edpb.europa.eu/our-work-tools/consistency-findings/opinions\\_en](https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en)



## Обзор от Bird&Bird по национальной специфике регулирования сферы Data Protection в ЕЭЗ

GDPR Tracker

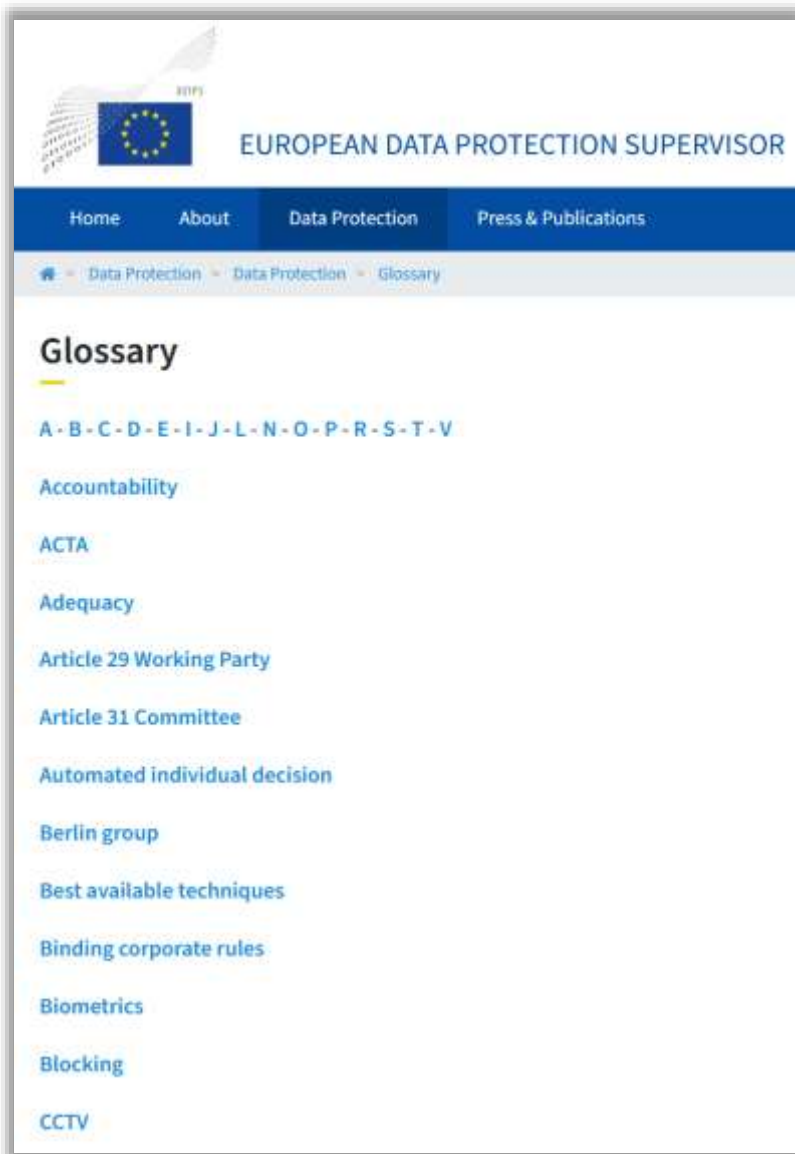
[Children online →](#)[Designation of a Data Protection Officer →](#)[Personal data of deceased persons →](#)[Employment →](#)[Genetic, biometric or health data →](#)[National identification numbers/any other identifier of general application →](#)[Any other areas under discussion →](#)[Approach to implementation →](#)[Timescale for implementation →](#)[Penalties →](#)[Personal data and freedom of expression →](#)[Professional secrecy →](#)[Scientific, historical or statistical purposes →](#)[Special rules for special categories of data →](#)[GDPR Tracker - Stage of legislative progress →](#)

## Архив материалов Global Privacy Assembly (International Conference of Data Protection and Privacy Commissioners)

The image shows a banner for the 43rd Assembly of Authorities of the Global Privacy Assembly. The banner features the GPA logo (a globe with a circular arrow) and the text "GPA Global Privacy Assembly (43<sup>rd</sup> Assembly of Authorities)". On the left, the logo for INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) is displayed. On the right, there is a vertical decorative strip with colorful geometric patterns and the text "18-21 OCT 2021". Below the banner, a text box states: "The Global Privacy Assembly first met in 1979 as the International Conference of Data Protection and Privacy Commissioners. The Assembly has been the premier global forum for data protection and privacy authorities for more than four decades."

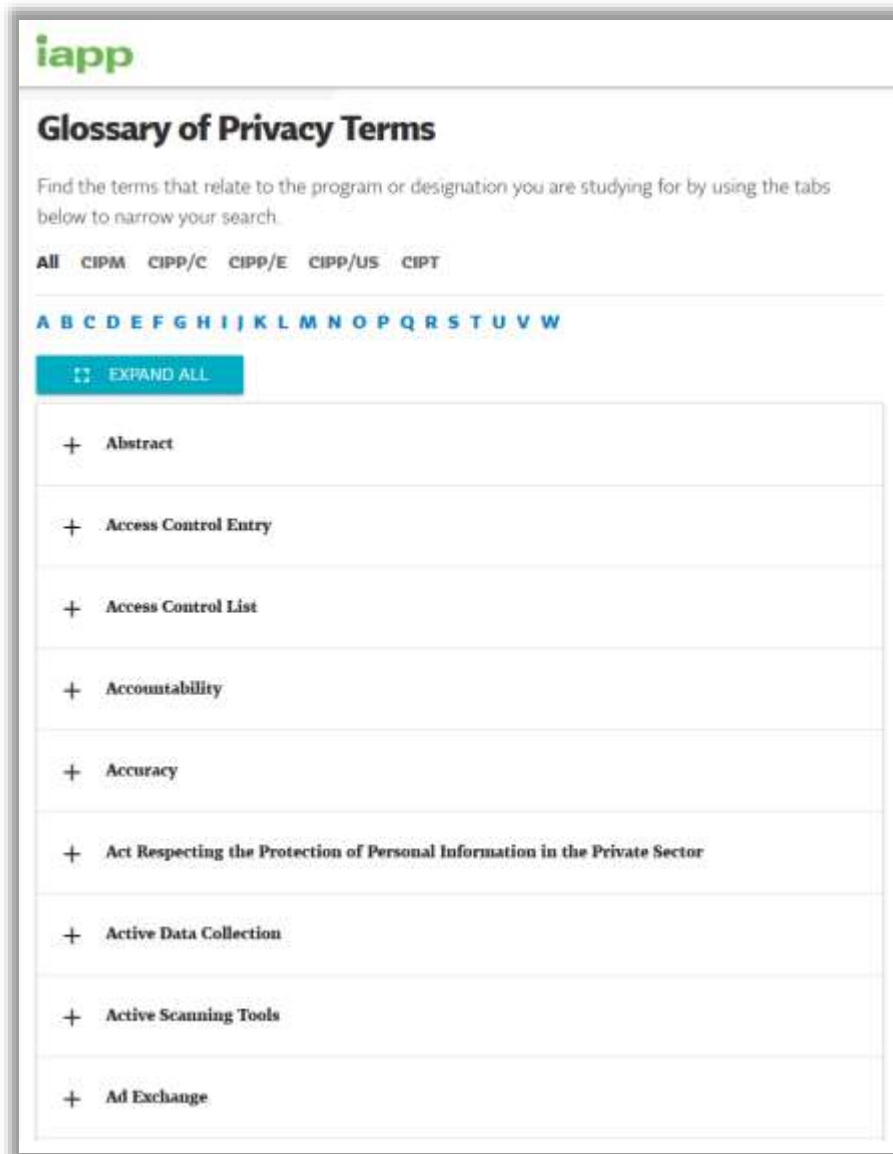
Решения и материалы Глобальной Ассамблеи Приватности (ранее известна как Международная конференция уполномоченных по защите данных и конфиденциальности), которая проводится на ежегодной основе с 1979 года под эгидой Европейского инспектора по защите данных ([European Data Protection Supervisor](https://edps.europa.eu/)).

## 27 Термины и определения в области data protection



The screenshot shows the EDPS website's glossary page. At the top left is the EDPS logo, which includes the European Union flag and the text 'EDPS'. To the right of the logo is the text 'EUROPEAN DATA PROTECTION SUPERVISOR'. Below this is a navigation bar with four tabs: 'Home', 'About', 'Data Protection', and 'Press & Publications'. The 'Data Protection' tab is selected. Below the navigation bar is a breadcrumb trail: 'Data Protection > Data Protection > Glossary'. The main heading is 'Glossary'. Below the heading is a list of letters: 'A - B - C - D - E - I - J - L - N - O - P - R - S - T - V'. Below the letters are several terms listed in blue text: 'Accountability', 'ACTA', 'Adequacy', 'Article 29 Working Party', 'Article 31 Committee', 'Automated individual decision', 'Berlin group', 'Best available techniques', 'Binding corporate rules', 'Biometrics', 'Blocking', and 'CCTV'.

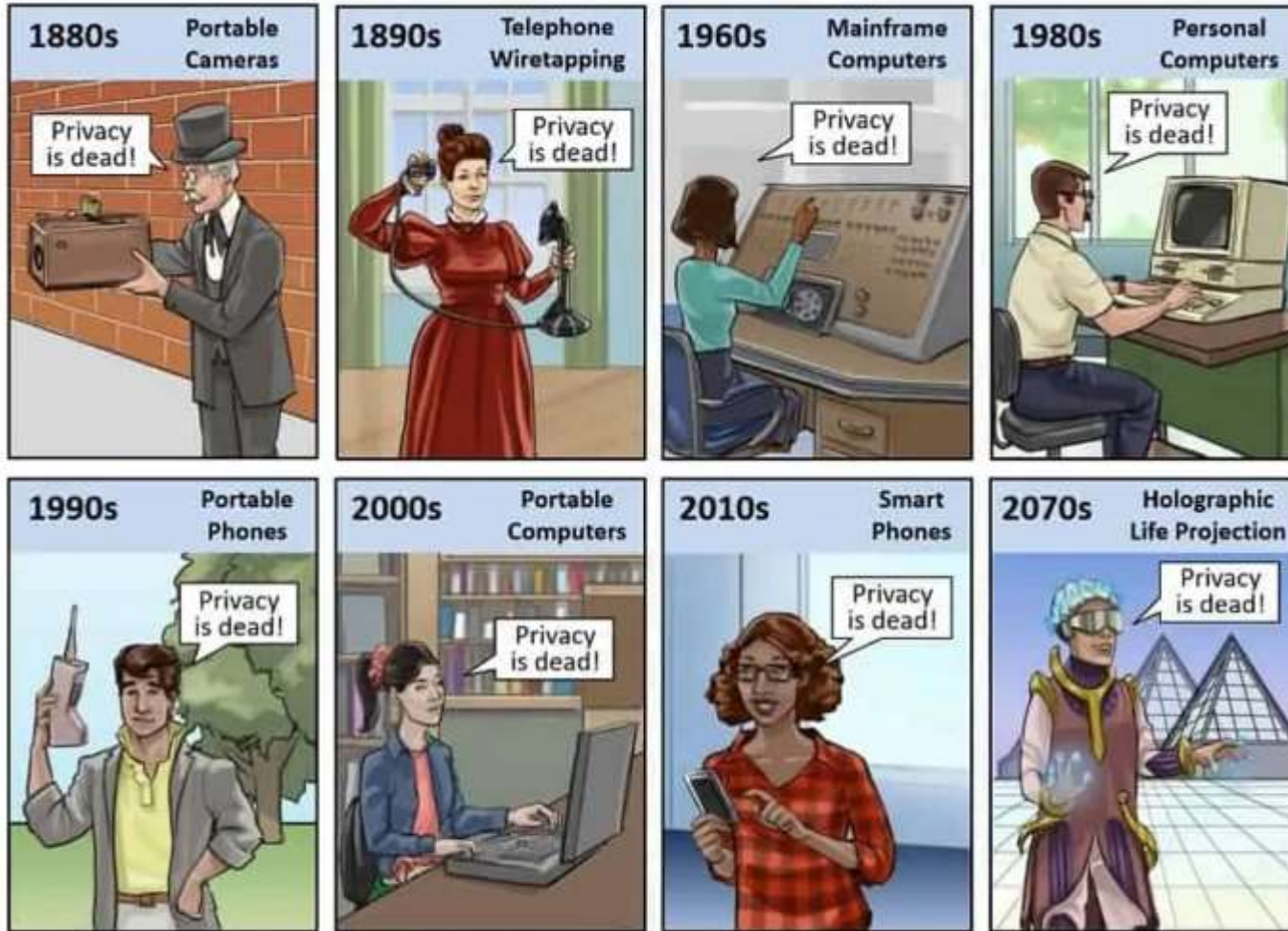
[https://edps.europa.eu/data-protection/data-protection/glossary\\_en](https://edps.europa.eu/data-protection/data-protection/glossary_en)



The screenshot shows the IAPP website's glossary page. At the top left is the IAPP logo. Below the logo is the heading 'Glossary of Privacy Terms'. Below the heading is a paragraph: 'Find the terms that relate to the program or designation you are studying for by using the tabs below to narrow your search.' Below the paragraph are several tabs: 'All', 'CIPM', 'CIPP/C', 'CIPP/E', 'CIPP/US', and 'CIPT'. Below the tabs is a row of letters: 'A B C D E F G H I J K L M N O P Q R S T U V W'. Below the letters is a button that says 'EXPAND ALL'. Below the button is a list of terms, each preceded by a plus sign: 'Abstract', 'Access Control Entry', 'Access Control List', 'Accountability', 'Accuracy', 'Act Respecting the Protection of Personal Information in the Private Sector', 'Active Data Collection', 'Active Scanning Tools', and 'Ad Exchange'.

<https://iapp.org/resources/glossary/>

# Персональные данные, принципы обработки и права субъектов



Written by Daniel J. Solove

Illustrated by Ryan Beckwith

For personal use only. Please ask us for permission for other uses.

[К оглавлению](#)



### **ANY INFORMATION**

Objective (earns 10k per year); Subjective (opinion); and, Sensitive data (gay woman).



### **RELATING TO**

An individual, about a particular person, impacts a specific person.



### **IDENTIFIED OR IDENTIFIABLE**

Direct or indirectly e.g. You know me by name, direct, you know me as "a Lawyer doing these graphics", indirect.



### **NATURAL PERSON**

applies ONLY to a living human being. National Law may give rules for deceased persons.



### **ONLINE IDENTIFIER & LOCATION DATA**

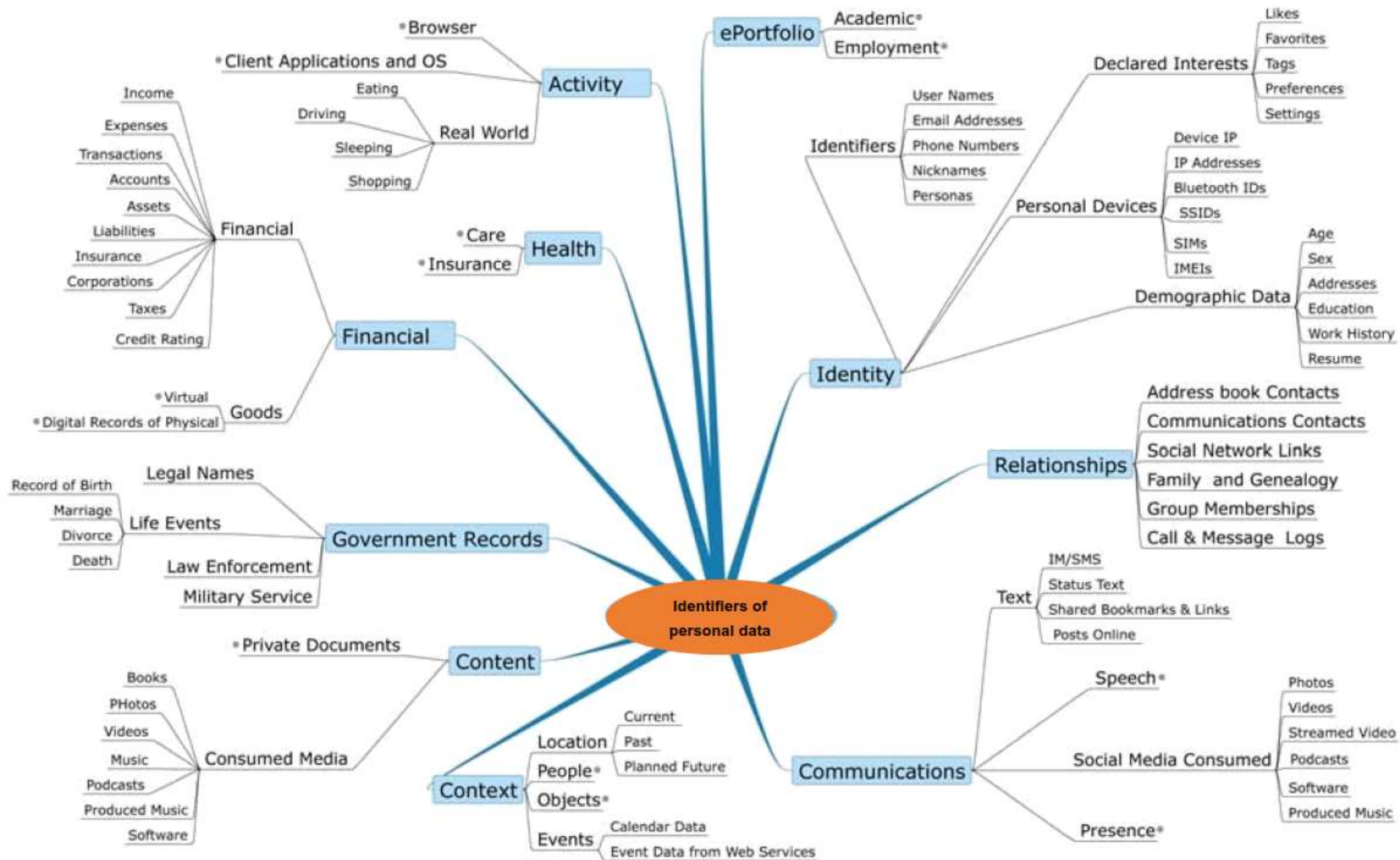
Include data provided by the electronic devices we use: mobiles, cookies identifiers, IP address, others.



### **TO ONE OR MORE FACTORS**

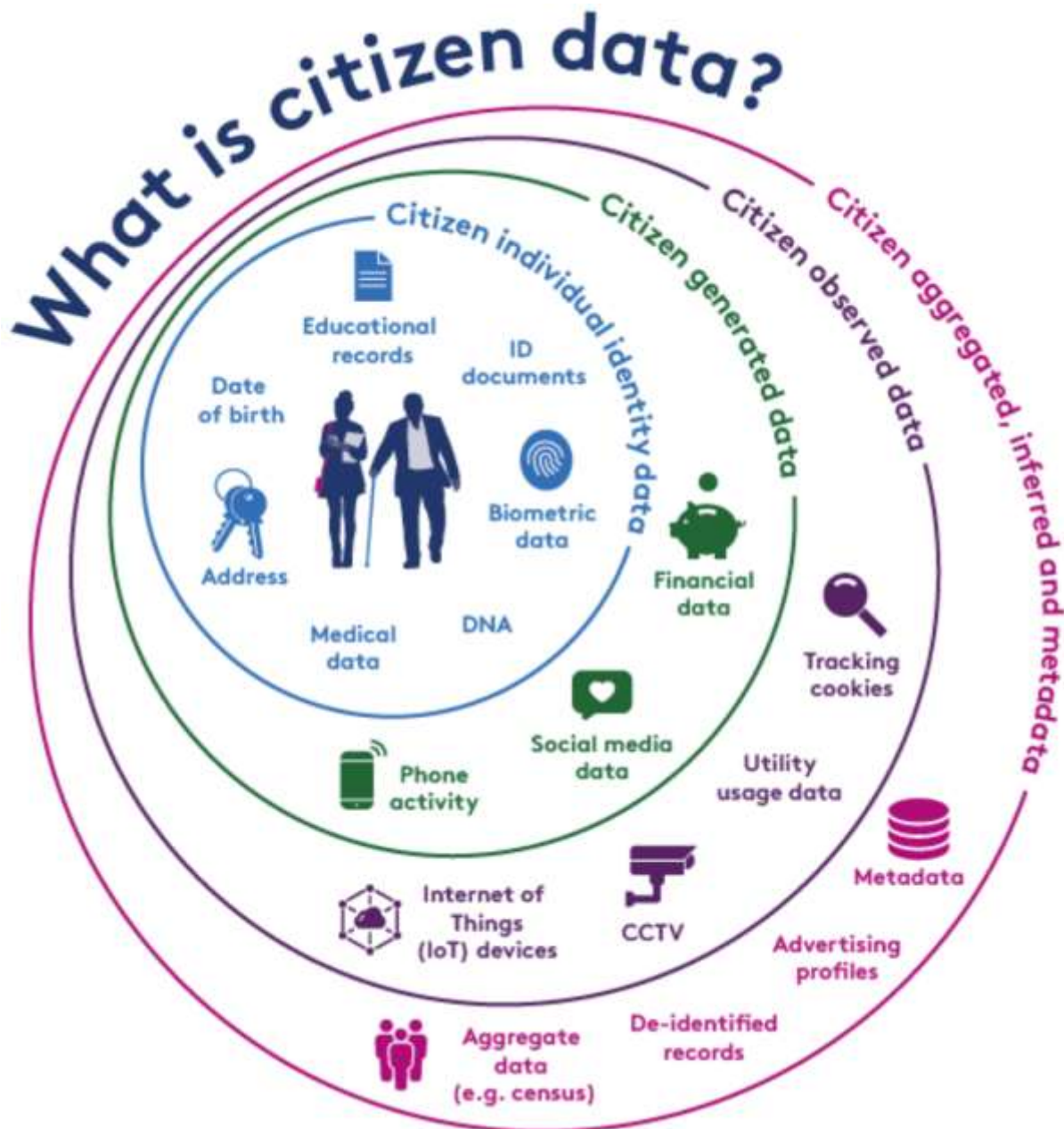
Include data that when combined with unique identifiers and other info create a profile and identify a person.

## 30 Пример категоризации персональных данных (1)



## 31 Пример категоризации персональных данных (2)











## 35 Принципы GDPR



### Законность, Справедливость, Прозрачность

Есть правовое основание на такую обработку  
Субъекты информируются о том, что их ПДн будут обрабатываться  
Информация ясная, краткая и простая для понимания, предоставляется в доступной форме



### Ограниченность целей обработки

Обработка ПДн с определенными, конкретными и законными целями



### Минимизация объемов обрабатываемых ПДн

Обработка ПДн осуществляется в объеме, необходимом для достижения целей обработки ПДн



### Точность и актуальность данных

Оператор и обработчик оценивают, насколько надежен источник получения ПДн, а также проявляют дополнительную осторожность, когда потенциальная неточность ПДн может иметь неблагоприятные последствия для субъекта ПДн



### Ограничение сроков хранения

Хранение ПДн не дольше, чем это необходимо для целей обработки ПДн



### Целостность и конфиденциальность

Обеспечивается соответствующая защита ПДн



Компания должна быть способна продемонстрировать свое соответствие требованиям GDPR

**Подотчетность**

## Принципы GDPR в сравнении с Конвенцией СЕ №108 и 152-ФЗ «О персональных данных»

Конвенция Совета Европы	GDPR	152-ФЗ
Законность	Законность, справедливость, <b>прозрачность</b>	Законность, справедливость
Справедливость, прозрачность		
Ограниченность целей	Ограниченность целей	Ограниченность целей
Адекватность и избыточность по отношению к целям	<b>Минимизация</b> данных	Неизбыточность по отношению к целям
Точность и актуальность	Точность и актуальность	Точность, актуальность, <b>достаточность</b>
Ограниченность времени хранения	Ограниченность времени хранения	Ограниченность времени хранения
-	<b>Подотчётность</b>	-
-	<b>Безопасность обработки</b>	-

## 37 Человеческие принципы обработки персональных данных

◇ Имейте мужество сказать своим клиентам, какого черта вы делаете с их данными и зачем... Надеюсь, у вас есть законная цель. Если нет... не беспокойтесь об остальном. **#прозрачность #подотчетность**

◇ Расскажите о своих целях понятным языком, не прячьтесь за юридическую чушь, вроде «например, но не ограничиваясь... бла, бла, бла». **#прозрачность**

◇ Будьте как можно более конкретными. Не используйте в качестве причины обработки персональных данных на вашем ресурсе фразу «Для улучшения пользовательского опыта...». Этому все равно никто не поверит. **#справедливость #законность**

◇ Если вы просто хотите расширить обработку данных, позвольте клиентам самим решить, интересно ли им это. Они доверились вам для достижения конкретной цели. Для других целей вы должны заслужить их доверие и/или согласие. **#ограничение\_обработки**

◇ Также дайте клиентам знать, когда и почему вы делитесь клиентскими данными с другими или получаете клиентские данные не от них самих. **#прозрачность #ограничение\_обработки**

◇ Не откусывайте больше, чем можете (или вам разрешено) проглотить. Если вам не нужны данные, например, для предоставления услуг, то не просите их. **#минимизация\_данных**

◇ Заботьтесь о клиентских данных, как о своих собственных... или даже лучше. Но не все данные одинаковы. Некоторые из них более чувствительны, чем другие. У всех нас есть «секреты». Храните «секреты» клиентов надежно, раз уж они поделились ими с вами. **#честность #конфиденциальность**

◇ Храните данные так, чтобы они были точными, актуальными и доступными. Не становитесь «складом» или «кладбищем» данных. Когда от каких-то данных нет практической пользы... избавьтесь от них. **#качество\_данных #ограничение\_хранения**

◇ Расскажите клиентам, какие данные о них хранятся на текущий момент. Они заслуживают того, чтобы знать. Если вы им не нравитесь... или ваши услуги, отпустите их. Не настаивайте! Отпустите их, если они хотят... и никогда больше не беспокойте их. **#справедливость #прозрачность**

◇ Если что-то случилось с данными клиентов, несмотря на все ваши усилия (вы знаете, что де\*\*мо случается), и это может стать для них плачевным, дайте им знать, прежде чем они столкнутся с проблемами. **#честность**

Права субъектов ПД



Информирование и доступ к ПД - позволяет получать сведения о цели, источниках, правовых основаниях, участниках, способе и сроках обработки ПД, а также получать уведомления о передаче ПД третьим лицам и об утечках ПД.



Переносимость ПД - позволяет получать копию ПД в формате, дающим возможность повторно использовать копию ПД в других сервисах/компаниях.



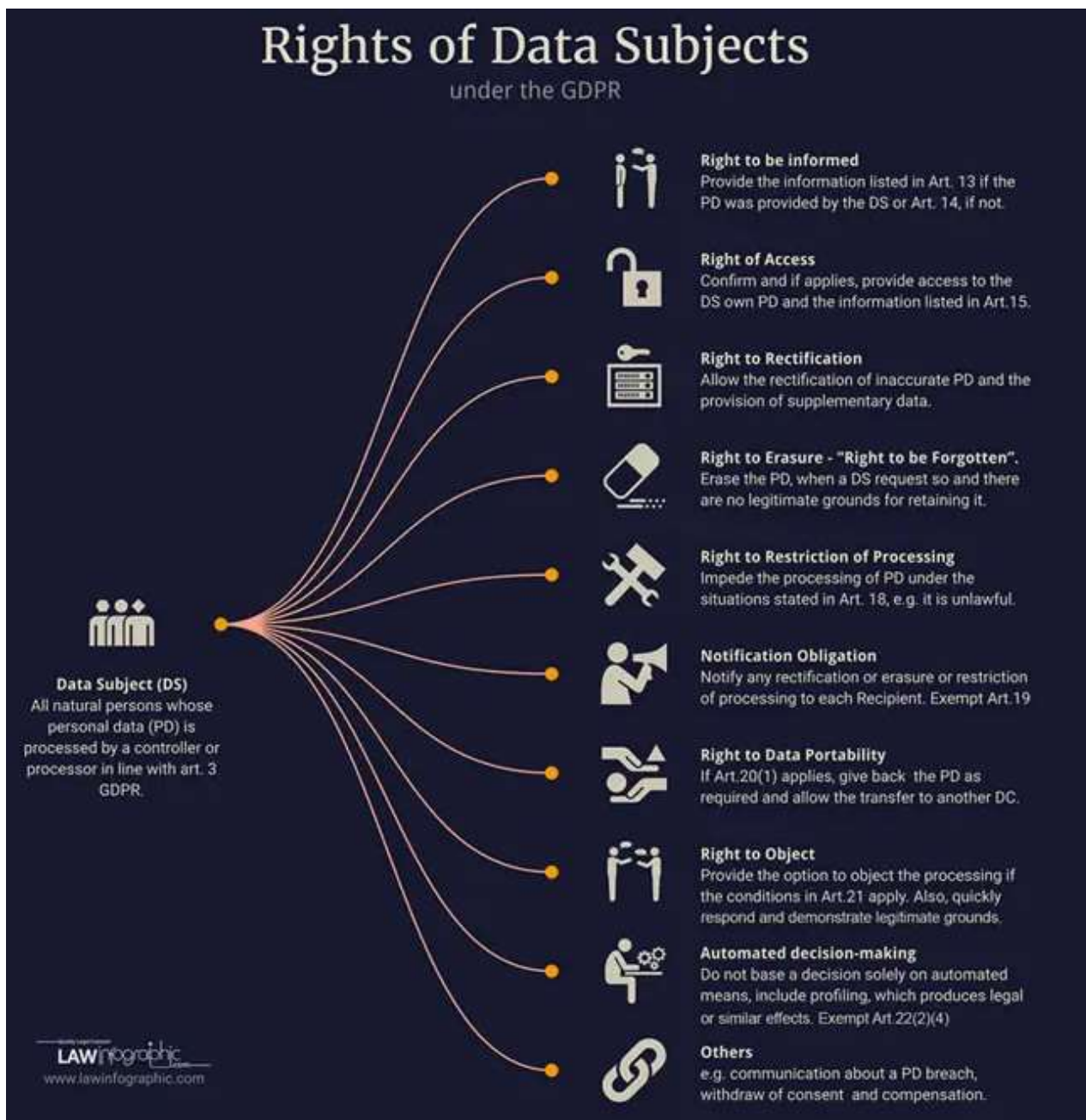
Возражение против обработки ПД - позволяет ограничивать прямые маркетинговые/рекламные контакты и возражать против решений, основанных на исключительно автоматизированной обработке ПД.



Прекращение обработки ПД (право быть забытым) - позволяет прекратить любую обработку ПД, которую нельзя обосновать договором с субъектом ПД или требованием закона.

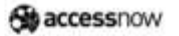


Исправление, блокирование, уничтожение ПД - позволяет требовать уточнения, блокирования или уничтожения неполных, устаревших, неточных, избыточных или незаконно полученных ПД.





## WHAT YOU WILL LEARN IN THIS GUIDE



### ● Introduction

GDPR, the new data protection law

### ● What is the General Data Protection Regulation?

Protecting **your personal data rights** in the European Union

What are  
my rights?

#### THE RIGHT TO

- ▶ information
- ▶ access
- ▶ rectification
- ▶ restrict processing
- ▶ erasure
- ▶ object
- ▶ an explanation
- ▶ data portability

How can I  
exercise  
my rights?



ENTITIES HOLDING  
MY DATA



What to do if my rights are  
**violated** and my data **misused**?

file a **complaint**

file a **case in court**

get **NGO representation**

### ● Conclusion

Take control, exercise your rights!



## 41 Больше прав для субъектов данных в GDPR

- Право на защиту данных (Rec.1, Art.1)
- Право распоряжаться своими данными (Rec.7)
- Право в любое время отозвать согласие на обработку данных (Art.7)
- Право на информацию и транспарентность в отношении обработки данных (Art.12-14, 19, 23)
- Право на доступ к данным (Art.15)
- Право на внесение исправлений в данные (Art.16)
- Право на удаление данных (Art.17)
- Право на ограничение обработки данных (Art.18)
- Право на переносимость данных (Art.20)
- Право на возражение против обработки данных (Art.21)
- Право не подчиняться решению, основанному на автоматизированной обработке данных (Art.22)
- Право быть уведомленным об утечке данных (Art.34)
- Право на обращение к Data Protection Officer (Art.38)
- Право на обращение (подачу жалобы) к надзорному органу (Art.77)
- Право на эффективные средства судебной защиты против надзорного органа (Art.78)
- Право на эффективные средства судебной защиты в отношении контролера или обработчика (Art.79)
- Право на представительство (передачу полномочий) (Art.79)
- Право на компенсацию материального или нематериального ущерба (Art.82)

## Права субъектов персональных данных в GDPR по сравнению с Конвенцией СЕ №108 и 152-ФЗ «О персональных данных»

152-ФЗ	Конвенция Совета Европы и GDPR
доступ к данным	комплекс прав из 152-ФЗ +
уточнение, блокирование, уничтожение данных	
ограничение прямых контактов с помощью средств связи для продвижения продукции или политической агитации	ограничение обработки данных
возражение против решений, основанных на исключительно автоматизированной обработке данных	возражение против обработки данных
обжалование действий или бездействия оператора	получение информации о нарушении безопасности данных
забвение ("право быть забытым")	переносимость данных
возмещение убытков и компенсация морального вреда	

◇ Это люди, такие же как и вы, а не просто «субъекты персональных данных»! Старайтесь почаще ставить себя на место человека, который доверил вам свои данные. **#гуманизм**

◇ Именно людям принадлежат их данные, а вам их дали просто подержать... какое-то время. Ваши права на данные закачиваются там, где начинаются права их естественных владельцев. **#справедливость #законность**

◇ Необходимо своевременно и доходчиво рассказывать людям о том, что происходит с их данными. Это даст им возможность полноценно распоряжаться своими данными и избегать многих проблем, а неизвестность порождает у людей недоверие и страх. **#честность #информирование**

◇ Некоторые люди руководствуются принципом "доверяй, но проверяй" и могут запросить у вас доступ к своим данным. И вам придется его предоставить... бесплатно :( Только, пожалуйста, не давайте одному человеку доступ к данным другого человека – ему это точно не понравится! **#прозрачность #доступ**

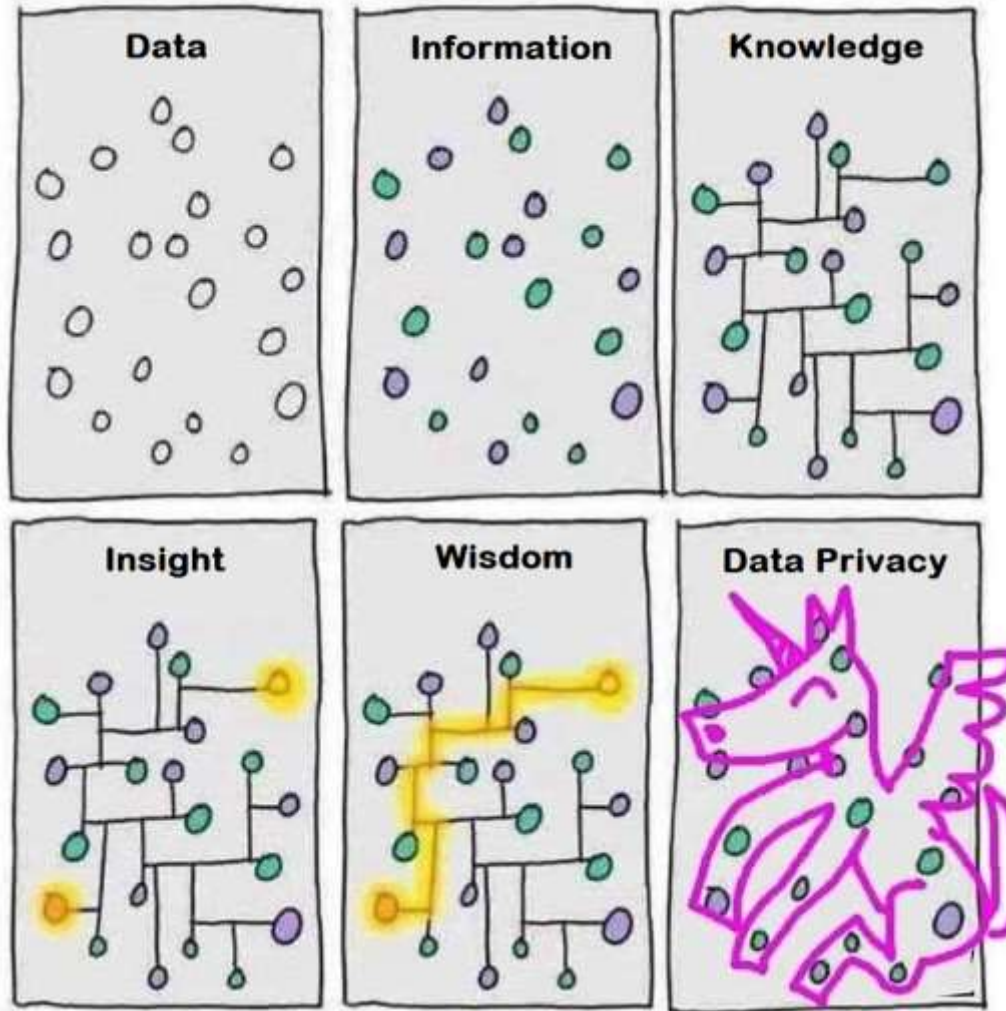
◇ Если ваше имя или фамилию хотя бы иногда путают, вы поймете всю боль человека, которому вы не даете исправить ошибки в его данных. Помните, что Влад не хочет быть Вадимом. **#качество\_данных #исправление**

◇ Иногда нам нужно отдохнуть друг от друга, верно? Любой человек по разным причинам может воспользоваться своим «правом на забвение» и попросить вас удалить некоторые или даже все данные о себе. Конечно, вы можете посулить ему «золотые горы» и попробовать переубедить, но не удивляйтесь, если этот человек попросит вас заблокировать его данные – хотя бы на время переговоров. **#минимизация\_данных #блокировка**

◇ Признайтесь, ведь вас тоже раздражает спам (телефонный в особенности) и нервирует ситуация, когда очередной банковский «искусственный интеллект» единолично ставит ипотечный крест на ваших мечтах об улучшении жилищных условий. Поэтому каждый может возражать против неприемлемой обработки своих данных. **#возражение #гуманизм**

◇ Не стоит превращаться в «тюрьму» для персональных данных. Не пытайтесь привязать к себе людей, используя их данные вместо цепей. Отпустите их, если они хотят... И дайте им возможность получить копию своих данных для повторного использования в других сервисах. **#переносимость\_данных**

# Accountability и демонстрация соответствия



# Руководство ICO по реализации принципа подотчетности в GDPR посредством Accountability Framework

**ico.**  
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters For organisations Make a complaint Action we've taken

## At a glance

Accountability is one of the key principles in data protection law – it makes you responsible for complying with the legislation and says that you must be able to demonstrate your compliance.

The Accountability Framework can help any organisation, whether small or large, with their obligations.

The framework is divided into 10 categories and contains expectations and examples of how your organisation can demonstrate your accountability.

As a starting point, we'd advise reading the Guide to the GDPR section on [accountability](#) first.

### Categories

- Leadership and oversight
- Training and awareness
- Transparency
- Contracts and data sharing
- Records management and security
- Policies and procedures
- Individuals' rights
- Records of processing and lawful basis
- Risks and data protection impact assessments
- Breach response and monitoring

### Take a self-assessment

The [accountability self-assessment](#) will help you to assess the extent to which your organisation is currently meeting the ICO's expectations in relation to accountability.

Accountability Framework – demonstrate your data protection compliance

Introduction to the Accountability Framework

Leadership and oversight

Organisational structure

Whether to appoint a DPO

Appropriate reporting

Operational roles

Oversight groups

Operational group meetings

Policies and procedures

Direction and support

Review and approval

Staff awareness

Data protection by design and by default

Training and awareness

All-staff training programme

Induction and refresher training

Specialised roles

Monitoring

Awareness raising

Individuals' rights

Informing individuals and identifying requests

Resources

Logging and tracking requests

Timely responses

Monitoring and evaluating performance

Inaccurate or incomplete information

Erasure

Restriction

Data portability

Rights related to automated decision-making and profiling

Individual complaints

Transparency

Privacy notice content

Timely privacy information

Effective privacy information

Automated decision-making and profiling

Staff awareness

Privacy information review

Tools supporting transparency and control

Records of processing and lawful basis

Data mapping

Record of processing activities (ROPA)

ROPA requirements

Good practice for ROPAs

Documenting your lawful basis

Lawful basis transparency

Consent requirements

Reviewing consent

Risk-based age checks and parental or guardian consent

Legitimate interest assessment (LIA)

Contracts and data sharing

Data sharing policies and procedures

Data sharing agreements

Restricted transfers

Processors

Controller-processor contract requirements

Processor due diligence checks

Processor compliance reviews

Third-party products and services

Purpose limitation

Risks and data protection impact assessments (DPIAs)

Identifying, recording and managing risks

Data protection by design and by default

DPIA policy and procedures

DPIA content

DPIA risk mitigation and review

Records management and security

Creating, locating and retrieving records

Security for transfers

Data quality

Retention schedule

Destruction

Information asset register

Rules for acceptable software use

Access control

Unauthorised access

Mobile devices, home or remote working and removable media

Secure areas

Business continuity, disaster recovery and back-ups

Breach response and monitoring

Detecting, managing and recording incidents and breaches

Assessing and reporting breaches

Notifying individuals

Reviewing and monitoring

External audit or compliance check

Internal audit programme


Performance and compliance information

Use of management information

<https://ico.org.uk/for-organisations/accountability-framework>

<https://ico.org.uk/media/for-organisations/accountability-framework-0-0.pdf>

## Структурное описание принципа подотчетности в GDPR на основе ICO Accountability Framework

Структурное описание принципа подотчетности в GDPR на основе ICO Accountability Framework  
v.1.0 2022.01.10 © Алексей Мунтян | Alexey Muntyan muntyan.alexey@gmail.com 

Согласно ст.5(2) GDPR контролёр несет ответственность за соблюдение принципов обработки ПД, зафиксированных в ст.5(1) GDPR, и должен быть в состоянии продемонстрировать его соблюдение («Принцип подотчетности»). В п.82 Преамбулы GDPR указано, что для демонстрации соответствия GDPR контролёр или процессор должен вести учет деятельности по обработке, за которую он отвечает. Каждый контролёр и процессор обязан сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение указанные учетные сведения в целях мониторинга процесса обработки.

Одним из наиболее проработанных и признаваемых в экспертной среде инструментов по созданию и поддержанию комплексной программы управления защитой ПД (Comprehensive Privacy Management Programme), а также по соблюдению принципа подотчетности, является Accountability Framework<sup>1</sup>, разработанный Офисом Уполномоченного по информации в Соединенном Королевстве (Information Commissioner's Office). На основе структуры и содержания указанного документа ниже описано 78 контролей (включая ссылки в себе около 360 элементов) подотчетности, сгруппированных в 10 категорий, где каждый из контролей направлен на обеспечение организацией возможности демонстрации соблюдения требований GDPR.

Данное описание не является дословным переводом на русский язык Accountability Framework, включает в себе несколько дополнительных контролей<sup>2</sup>, а также содержит нормативные ссылки и указания. Поданным переводом предоставлена документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR.

**Навигация:**

1. Руководство и надзор ..... 1
2. Политики и процедуры ..... 2
3. Обучение и осведомленность ..... 3
4. Права субъектов данных ..... 4
5. Прозрачность ..... 6
6. ИИ/ИИ и автоматизированные системы ..... 8
7. Создание и обмен данными ..... 10
8. Оценка рисков и DPIA ..... 13
9. Управление данными и безопасность ..... 15
10. Разрешение на обработку и экспорт ..... 18
- Документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR ..... 20
- Перечень сформированной и из размещенной ..... 21

**Описание контролей демонстрации соблюдения требований GDPR**

**1. Руководство и надзор**

Основной задачей элемента является эффективное руководство и надзор. Это включает в себя «внесение четкой ответственности» за деятельность, связанную с обработкой и защитой данных, на стратегическом и функциональном уровнях. В некоторых организациях по этому вопросу требуется должность CPO, но каждая организация должна выделить достаточные ресурсы и создать за тем, чтобы защита данных была общей ответственностью, а не задачей отдельного человека, непосредственно выполняющего функции по защите данных. Руководство организации должно нести свою долю ответственности за защиту данных, и оно должно поднимать пример прозрачности, легкости и доступности политики и защиты данных, который лежит в основе всего остального.

**3.1. Организация структуры**

Существует организационная структура для управления и практической реализации защиты данных, которая обеспечивает эффективное руководство и надзор, четкий порядок и обязанности, а также эффективные коммуникации.

**Обязанности**

- Руководство организации несет общую ответственность за управление и практическую реализацию защиты данных.
- Лица, принимающие решения, подает пример и поощряет культуру, конструктивную культуру соблюдения требований по защите данных.
- Существует четкая модель коммуникации между соответствующими группами.
- Политика и процедуры четко определяют организационную структуру управления и практической реализации защиты данных.
- В должностных инструкциях четко прописаны обязанности и порядок предоставления отчетности руководству.
- Должностная инструкция является детальной, соответствует поставленной цели и регулярна.
- Персонал, обеспечивающий защиту данных, понимает организационную структуру и свои обязанности.

**Ссылки**

- GDPR: ст.24, ст.74
- ICO's Guidelines (2020) on the concepts of controller and processor in the GDPR
- ICO's Guidelines on the concepts of controller, processor and joint controller under Regulation (EU) 2018/1725
- Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020)

**3.2. Контроль**

**Инициативы GDPR**

Согласно ст.5(2) GDPR контролёр несет ответственность за соблюдение принципов обработки ПД, зафиксированных в ст.5(1) GDPR, и должен быть в состоянии продемонстрировать его соблюдение («Принцип подотчетности»). В п.82 Преамбулы GDPR указано, что для демонстрации соответствия GDPR контролёр или процессор должен вести учет деятельности по обработке, за которую он отвечает. Каждый контролёр и процессор обязан сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение указанные учетные сведения в целях мониторинга процесса обработки.

Одним из наиболее проработанных и признаваемых в экспертной среде инструментов по созданию и поддержанию комплексной программы управления защитой ПД (Comprehensive Privacy Management Programme), а также по соблюдению принципа подотчётности, является [Accountability Framework](https://rppa.ru/analytika/accountability-framework), разработанный Офисом Уполномоченного по информации в Соединенном Королевстве (Information Commissioner's Office). На основе структуры и содержания указанного документа ниже описано **78 контролей (включающих в себя около 360 элементов) подотчетности, сгруппированных в 10 категорий**, где каждый из контролей направлен на обеспечение организацией возможности демонстрации соблюдения требований GDPR.

Данное описание не является дословным переводом на русский язык Accountability Framework, включает в себя несколько дополнительных контролей, а также содержит нормативные ссылки. Отдельным перечнем приведена документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR.

# Проект стандарта EN 17529. Personal data protection requirements for processing operations

oSIST prEN 17799:2022

EUROPEAN STANDARD **DRAFT**  
 NORME EUROPÉENNE **prEN 17799**  
 EUROPÄISCHE NORM

December 2021

---

ICS 03.120.20; 03.160

English version

**Personal data protection requirements for processing operations**

Exigences de protection des données à caractère personnel pour les opérations de traitement
Anforderungen an den Datenschutz bei Verarbeitungsvorgängen

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.



If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation. Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

**Warning:** This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

CEN-CENELEC Management Centre:  
Rue de la Science 23, B-1040 Brussels

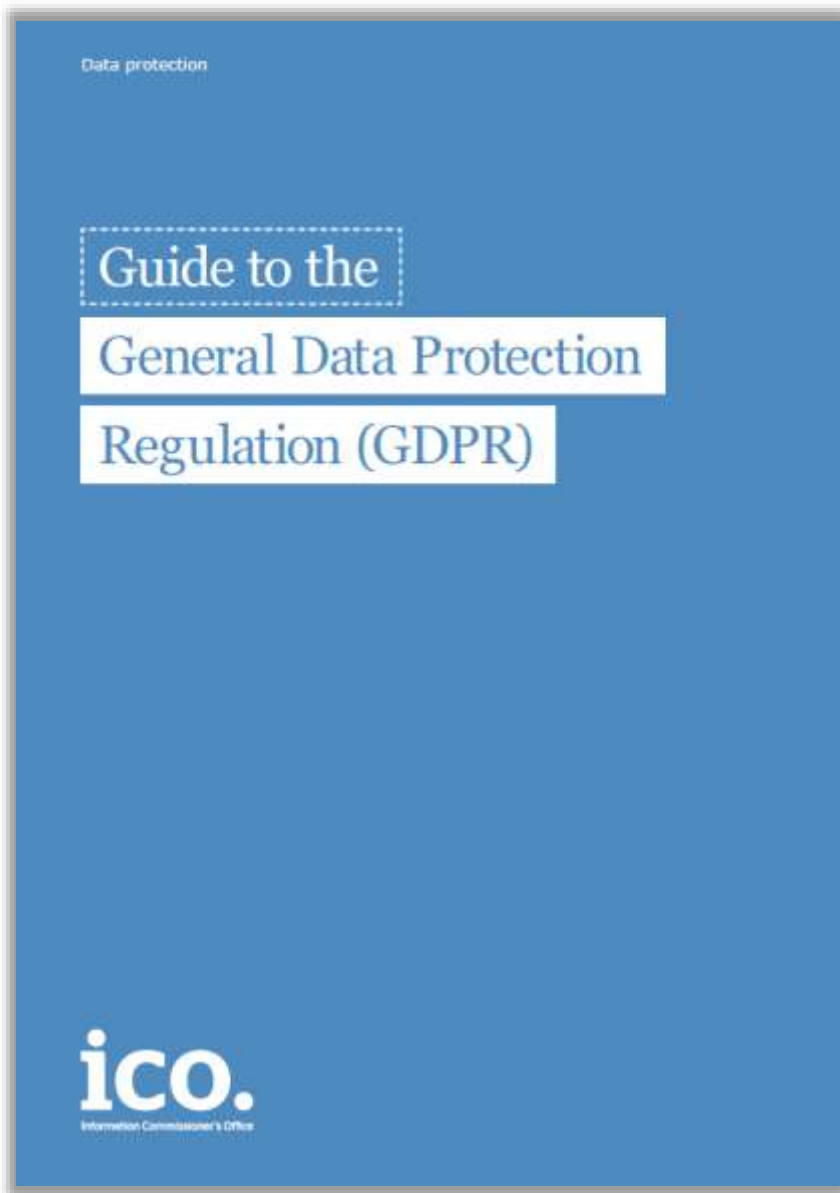
---

© 2021 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members. Ref. No. prEN 17799:2021 E

Европейский комитет по стандартизации CEN готовит проект стандарта EN 17529 «Personal data protection requirements for processing operations».

Документ устанавливает базовые требования к демонстрации соответствия деятельности по обработке персональных данных европейской нормативной базе по защите персональных данных, в соответствии со стандартом EN ISO/IEC 17065.

Стандарт применим в любых организациях, которые обрабатывают персональные данные в качестве контролёров и/или процессоров данных и его цель заключается в том, чтобы предоставить набор требований, позволяющих таким организациям эффективно обеспечивать соответствие европейской нормативной базе по защите персональных данных. Организация может принять решение о том, что стандарт применим только к определенному подмножеству её деятельности по обработке персональных данных, если такое решение не влечёт за собой несоответствие европейской нормативной базе по защите персональных данных.



About the Guide to the GDPR	3
What's new	4
Key definitions	8
What is personal data?	9
Controllers and processors	13
Principles	17
Lawfulness, fairness and transparency	19
Purpose limitation	23
Data minimisation	27
Accuracy	32
Storage limitation	39
Integrity and confidentiality (security)	47
Accountability principle	48
Lawful basis for processing	49
Consent	58
Contract	63
Legal obligation	66
Vital interests	69
Public task	72
Legitimate interests	76
Special category data	82
Criminal offence data	87
Individual rights	91
Right to be informed	92
Right of access	100
Right to rectification	106
Right to erasure	113
Right to restrict processing	121
Right to data portability	129
Right to object	142
Rights related to automated decision making including profiling	151
Accountability and governance	157
Contracts	167
Documentation	170
Data protection by design and default	175
Data protection impact assessments	186
Data protection officers	194
Codes of conduct	202
Certification	208
Data protection fee	213
Security	214
Encryption	227
Passwords in online services	231
Personal data breaches	242
International transfers after the UK exit from the EU Implementation Period	251
Standard Contractual Clauses (SCCs) after the transition period ends	267
Exemptions	269
Immigration exemption	299



# RGPD

## PASSER À L'ACTION

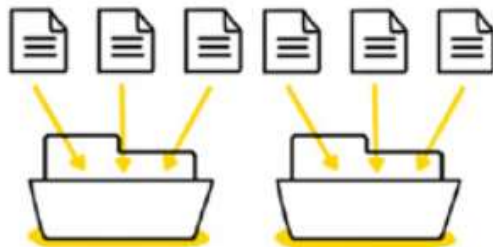
en 4 étapes

1



Constituez un registre de vos traitements de données

2



Faites le tri dans vos données

3



Respectez les droits des personnes

4



Sécurisez vos données

## Онлайн-сервис от AEPD для подготовки документов для выполнения требований GDPR



The screenshot shows the website for 'Facilita EMPRENDE' by the Spanish Data Protection Agency (AEPD). The page title is 'Facilita EMPRENDE'. Below the title, there is a brief description: 'This new tool seeks to support entrepreneurs and start-ups the processing activities what involve strong innovative features and the use of new technologies.' There are social media icons for Facebook and Twitter. The main content is a list of documents generated by the tool, including a two-tiered information policy, pre-printed Records of Processing Activities (RAT), an incident record form, contractual clauses, a cookie policy, and recommendations for managing security breaches and digital harassment.

**Facilita EMPRENDE**

This new tool seeks to support entrepreneurs and start-ups the processing activities what involve strong innovative features and the use of new technologies.

Much in the same way as FACILITA – RGPD, FACILITA – EMPRENDE is a free, user friendly tool based on a series of guided questionnaires that enable categorization of the types of processing carried out by the company. At the end of this execution, a series of adapted documents are provided to be used as guidelines and support in order to comply with obligations provided by applicable regulations on data protections. Specifically, the following will be obtained:

- A two-tiered information policy composed by the informative clauses to be provided at the time that data are collected, and a privacy policy;
- pre-printed Records of Processing Activities (RAT);
- the incident record form in order to comply with article 33.5 regarding the documents of security breaches that affect or may affect personal data;
- a set of contractual clauses to be included in any contacts subscribed with providers and data processors;
- if your company has a website featuring cookies or similar technologies, a cookie policy.
- a series of recommendations and guidelines in order to help you with the process of adaptation with regard to management of security breaches, assistance to the exercise of rights, recommendations on video surveillance, and specific instructions for the management of the risks associated to processing, as well as privacy strategies and security measures to be implemented.
- A series of recommendations to prevent digital harassment.

Испанский орган по защите данных, Agencia Española de Protección de Datos, объявил о запуске онлайн-сервиса под названием Facilita Emprende (есть версии на испанском и английском) для того, чтобы помочь малому бизнесу и стартапам с выполнением требований GDPR. Сервис работает на основе заполняемого опросника, с помощью которого будут автоматически генерироваться необходимые документы, включая политику конфиденциальности, политику использования файлов cookie, договорные условия о персональных данных и многое другое.

## Инструментарий «Boost» от бельгийского L'APD для обеспечения соответствия требованиям GDPR



Autorité de protection des données CITOÏEN FR

THÈMES VIE PRIVÉE AGIR PUBLICATIONS L'AUTORITÉ PRESSE Chercher

Actualités L'APD développe de nouveaux documents et outils pratiques

16 MARS 2021

### L'APD développe de nouveaux documents et outils pratiques

De nouveaux documents pratiques ont été élaborés pour les responsables du traitement, les sous-traitants et les DPO :

- modèle de registre des activités de traitement simplifié pour les responsables du traitement et les sous-traitants
- feuille de route pour les échanges de données personnelles par/avec les organismes publics fédéraux
- template de protocole de communication des données à caractère personnel (article 20, loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel)

Dans le cadre du projet Boost, l'APD a également développé des outils pour les PME :

- Brochure FAQ
- Guide condensé PME
- Modèles de lettres pour l'exercice des droits
- Vidéos animées

Découvrez tous les autres outils mis à disposition par l'APD dans notre [Toolbox](#).

Бельгийский орган по защите данных, Autorité de protection des données, опубликовал инструментарий под названием Boost (доступны нидерландский и французский языки) для того, чтобы помочь малому бизнесу и стартапам с выполнением требований GDPR. Инструментарий включает в себя краткое руководство по GDPR, образец реестра процессинговых активностей (RoPA), шаблон протокола передачи персональных данных (data portability) и иные документы.

## Практическое руководство NYMITY по демонстрации соответствия GDPR



### Awareness

According to many Data Protection Authorities, GDPR compliance starts with raising awareness on the requirements of the new law within an organisation. That way, the minds can be prepared for the work to be done, including the reasons why an organisation may have a new or renewed focus on privacy and data protection.



### Inventory / Article 30 Register

This is the same requirement as described above under the "Governance Approach". Many DPAs agree that in order to have a good overview of what is going on in an organisation, the Processing Activities Register is a vital element. It will not only provide the overview of the ongoing data processing operations, but will also help organisations to decide which are the appropriate technical and organisational measures that need to be implemented. Furthermore, it supports the drafting or updating of privacy notices, which will need to include a lot of information already included in the Register. Last but not least, the information included in the Register allows to assess if processing activities are "high risk" and thus need to be part of a DPIA.



### Impact Assessments for key projects

All "high risk" processing operations, including those in which sensitive data are processed, need to undergo a data protection impact assessment. Organisations are free to decide if they wish to extend this obligation to more project. If a DPIA is completed, the organisation will make an inventory of the risks to the rights and freedoms of the data subject, including, but not limited to, privacy and data protection. These risks will subsequently need to be mitigated, for example by applying specific safeguards to a processing operation.



### Procedures for Data subject rights and breaches

Where they have not yet been established before, DPAs recommend to develop internal procedures on how to deal with the rights attributed to data subjects (including the right to information, access, rectification and erasure) and data breaches. Should procedures already be in place, they would in any case need to be reviewed to ensure they are in line with the requirements of the GDPR and, when available, the guidance of the Article 29 Working Party.



### Notice / Communication

The GDPR imposes strict obligations on the information to be provided to data subjects when their personal data is processed. That information shall be included in one, or multiple, privacy notices or statements, which need to be written in plain language. Organisations will need to review their current notices and/or draft new ones. The Processing Activities Register could help to include many details of the processing operation in the notice.



### Consent & other legal grounds

The DPAs remind organisations that all processing operations require one of six legal grounds: consent, performance of a contract, a legal obligation, a public interest, a vital interest of a data subject or other data subject, or a legitimate interest. Without any of these legal grounds, personal data cannot be legally processed. For each (purpose of) a processing operation, the applicable legal ground is to be documented. Furthermore, where legitimate interest or consent are being used, organisations should stand ready to provide further explanations on how these legal grounds apply in the specific situation and if the criteria imposed by the GDPR are met.



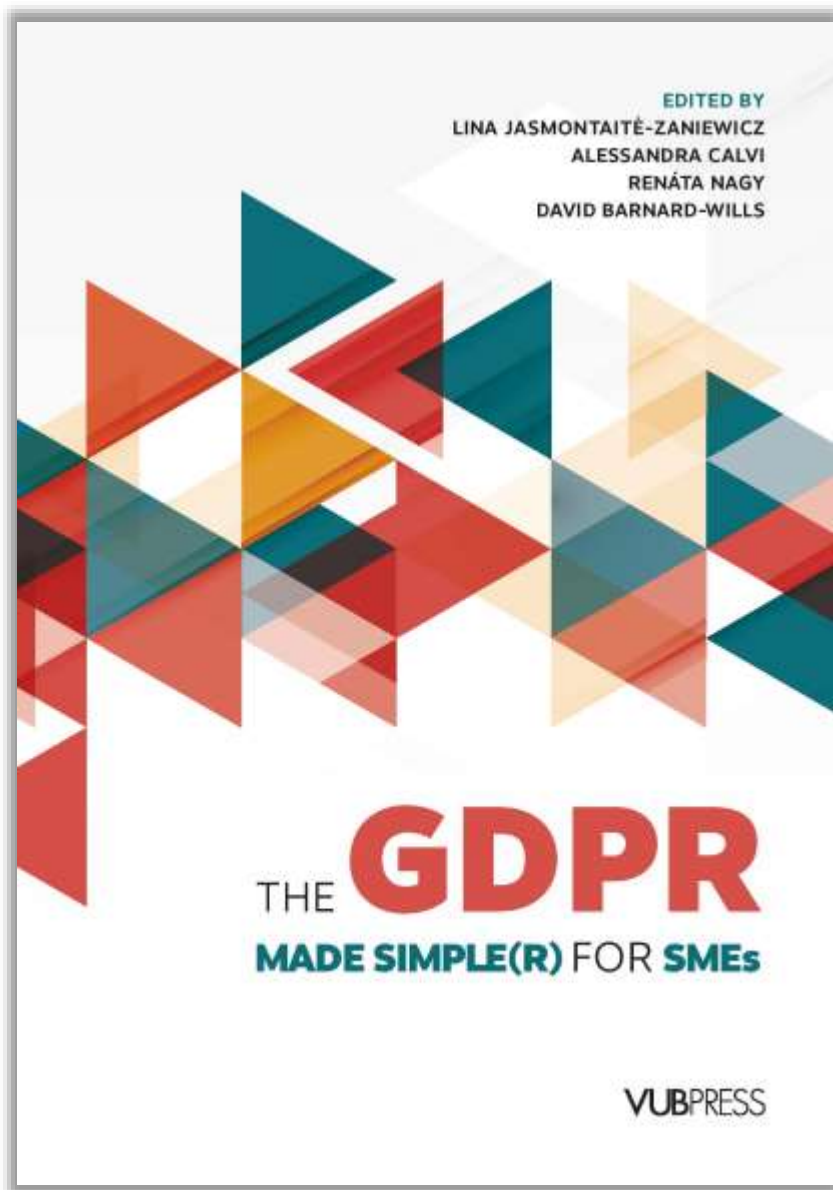
### Children

Although the GDPR does not contain many provisions on processing personal data of minor's, most DPAs recommend to take extra care when dealing with data from children. Organisations are recommended to put in place specific safeguards where possible. Also compliance with the minimum age for consent in an online environment, which may vary from 13 to 16 depending on the EU Member State, needs to be clearly documented.



### DPO

The final step recommended by most Data Protection Authorities is to verify whether a Data Protection Officer needs to be appointed. This is a prescribed role under the GDPR, for example for all public authorities and organisations that are processing sensitive data at a large scale.



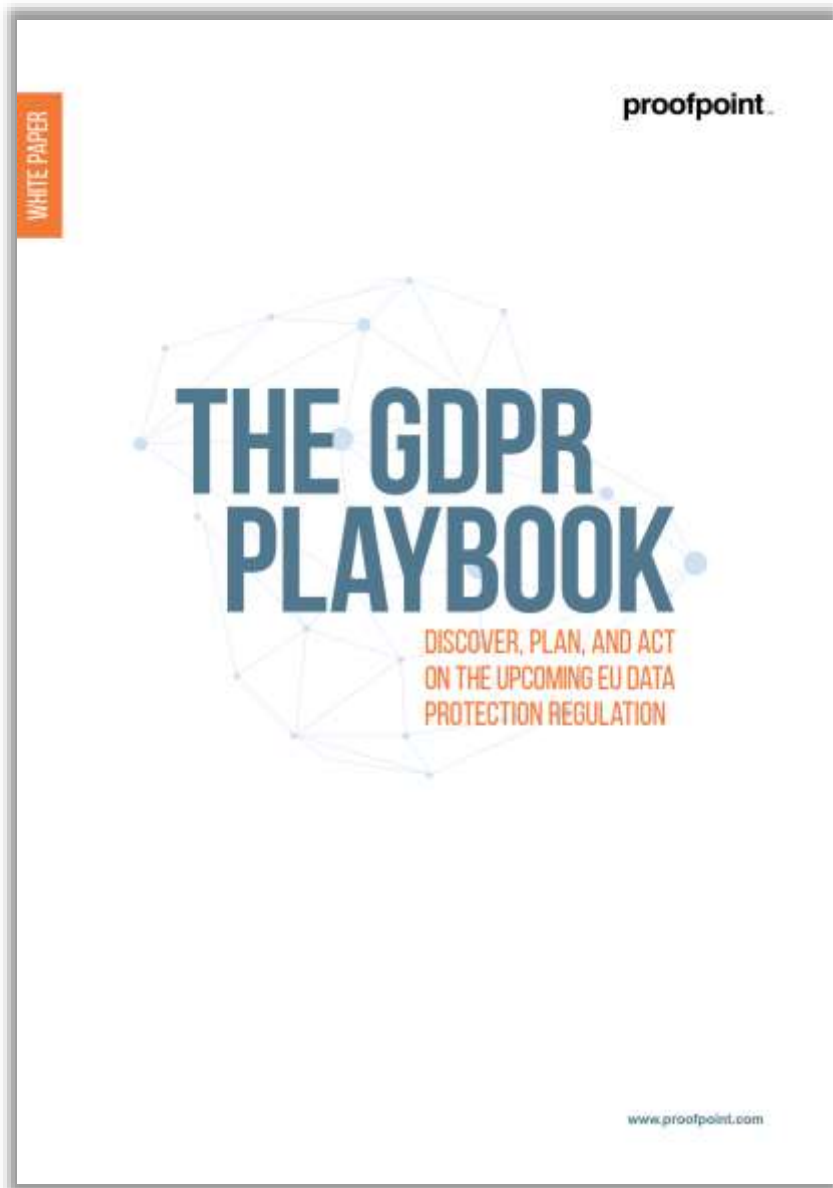
**EXAMPLE**

For qualitative risk assessment, an exemplary severity scale of 1-5 could be:<sup>162</sup>

Value	Severity of Impact on rights and freedom of data subjects
S1	Low - Mere inconvenience/Annoyance
S2	Moderate - Minor physical, material or non-material damage to rights and freedoms of data subjects (e.g. stress, feeling of loss of control of personal data, minor economic loss, etc.)
S3	Medium - Physical, material or non-material damage to rights and freedoms of data subjects (e.g. restrictions to exercising rights)
S4	High - Significant physical, material or non-material damage to rights and freedoms of data subjects that can only be overcome by data subjects with difficulty
S5	Critical - Irreversible physical, material or non-material damage to rights and freedoms of data subjects

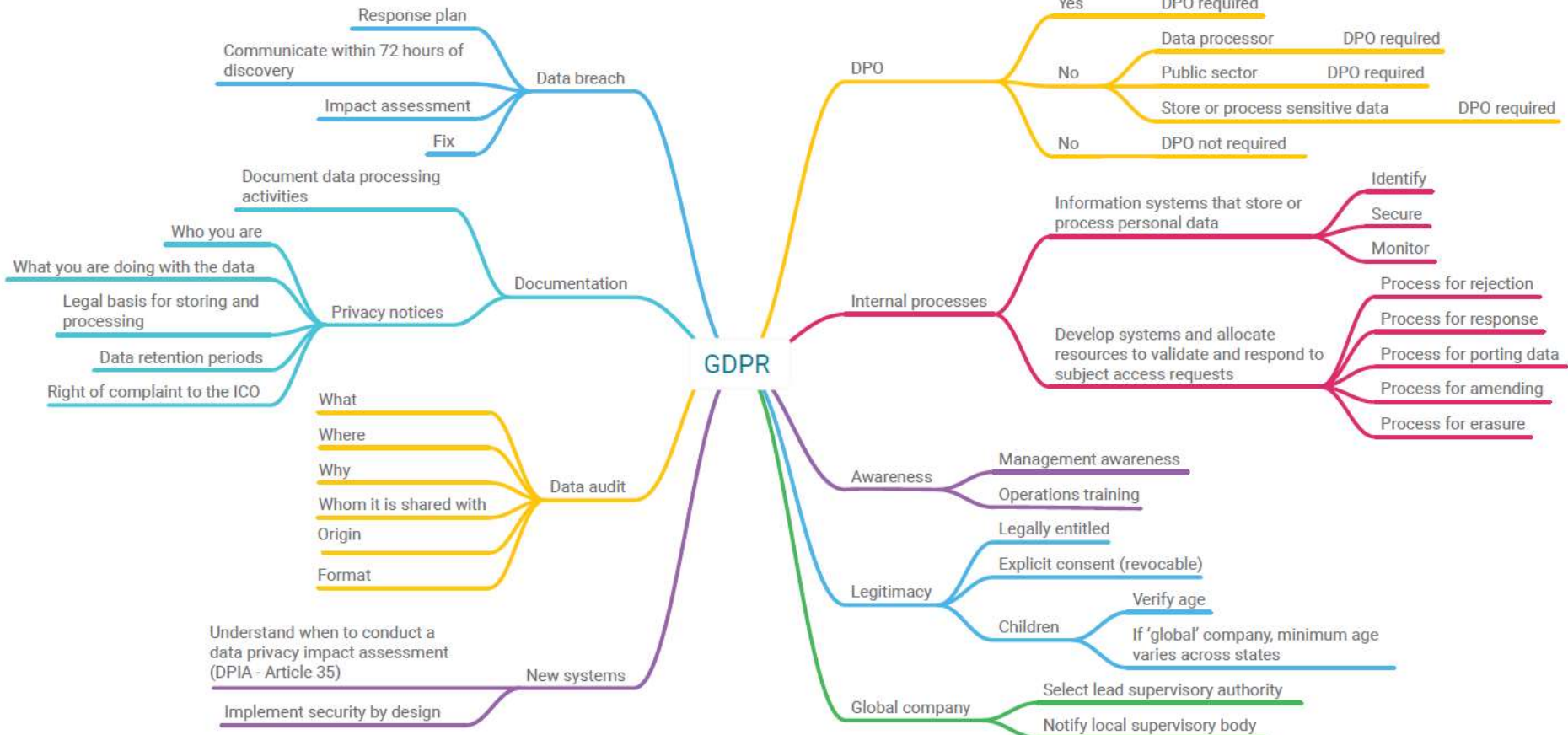
Whereas a likelihood scale 1-5 could be:<sup>163</sup>

Value	Likelihood of occurrence
L1	Remote - it does not seem possible that the selected risk sources will materialize
L2	Unlikely - it seems unlikely that the selected risk sources will materialize
L3	Occasional - it seems possible that the selected risk sources will materialize
L4	Likely - it seems highly possible that the selected risk sources will materialize
L5	Frequent - it is almost certain that the selected risk sources will materialize



<b>Understanding the GDPR: Seven Principles to Knows</b> .....	4
Principle 1: Lawfulness, Fairness, and Transparency .....	4
Principles 2 & 3: Accuracy and Purpose Limitation .....	4
Principles 4 & 5: Data Minimisation and Storage Limitation.....	4
Principle 6: Integrity and Confidentiality.....	4
Principle 7: Accountability.....	5
<b>Why the GDPR Matters: Accountability Will Drive Investment</b> .....	5
<b>Roadmap to Compliance: Data Governance is a Living, Breathing Process</b> .....	6
Step 1: Discover—Conduct a Data Audit.....	7
Step 2: Plan—Develop a Remediation Roadmap .....	8
<i>Policy creation drives changes in behaviour</i> .....	8
Step 3: Protect—Implement process and technology controls .....	8
Step 4: Enhance—Monitor Control Effectiveness with Regular Assessments .....	10
<b>The GDPR Compliance Checklist</b> .....	11
<b>Conclusions and Recommendations</b> .....	12

Key GDPR Domains and Requirements

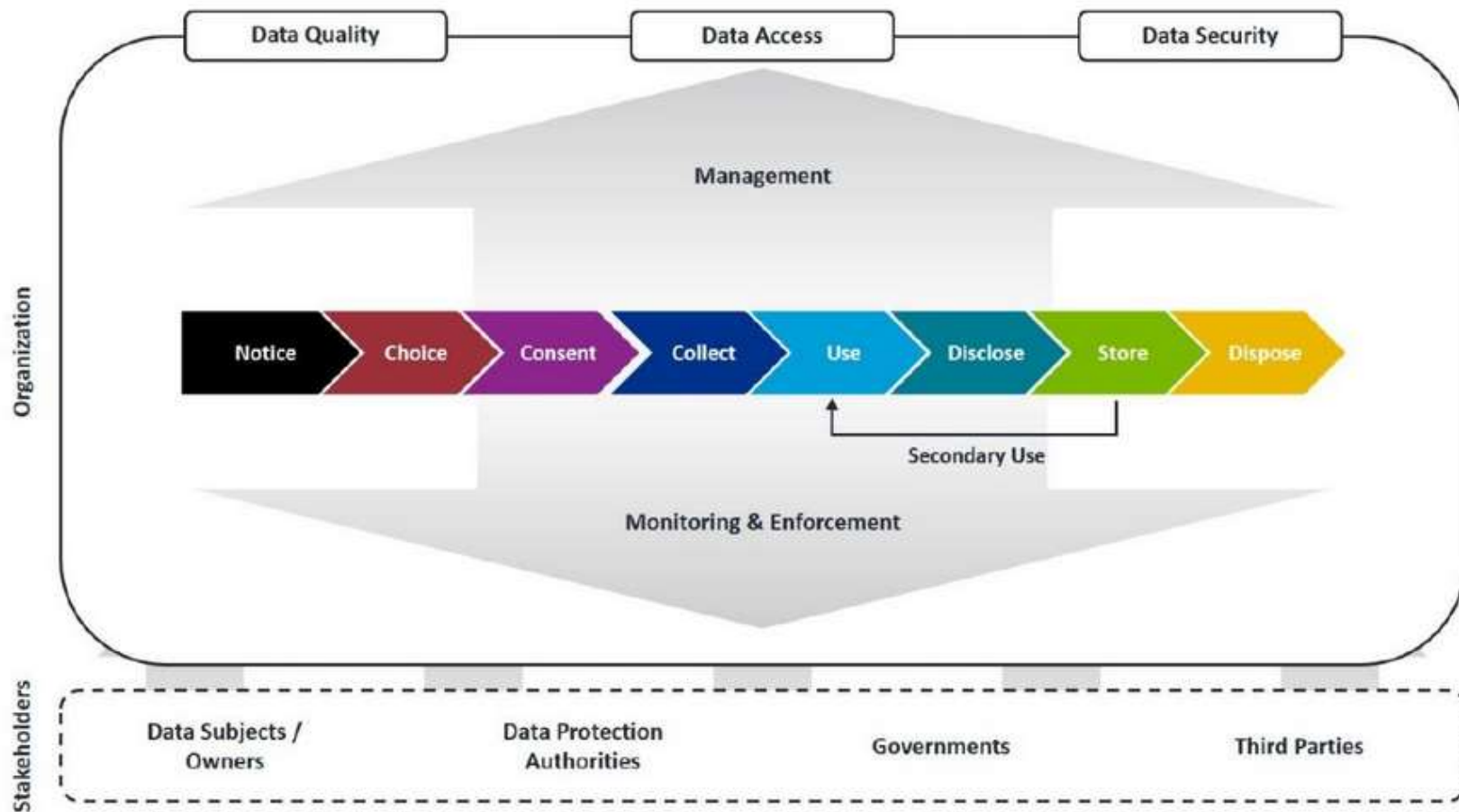


<https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoETEA0>

<https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9qEAC>

<https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoDuEAK>

## 56 Пособие NOREA по аудиту выполнения требований GDPR







**Gartner.**

# GDPR Audit Checklist

The Gartner GDPR Audit Checklist helps organizations prepare for internal and external audits of GDPR compliance.

**Instructions:**

1. Track the status of all checklist items until fully compliant.
2. Use the notes page as needed for comments on progress.

For each requirement we have noted the relevant GDPR article for easy reference.

**Get Started**

Status key						
FC - Fully compliant		IP - In progress		NC - Not compliant		NA - Not applicable
	Audit question	Reference article	Status			
Accountability governance	Do you maintain an overarching data protection policy that demonstrates compliance with requirements including processing, privacy by design and record keeping?	5(2)	FC	IP	NC	NA
	Do you train all employees on GDPR requirements and principles — including processing activities, controls, privacy impact assessments, audits, data subject rights, reporting lines and privacy by design — and the potential impact of noncompliance?	5(2)	FC	IP	NC	NA
	Do you regularly test, retrain and maintain records of training for employees who handle personal data on their understanding of GDPR requirements?	5(2)	FC	IP	NC	NA
	If you require a data protection officer (DPO), does he or she have reporting authority to the highest level of management, necessary resources, independence, and authority to ensure compliance with the GDPR and other data protection laws?	7(1) 38(1-4,6)	FC	IP	NC	NA
	Is the DPO bound by secrecy or confidentiality concerning the performance of his or her tasks?	38(5)	FC	IP	NC	NA
	If the DPO has other responsibilities, have they been assessed to avoid conflicts of interest?	38(6)	FC	IP	NC	NA
	Does the DPO have the knowledge and ability to fulfill tasks outlined in Article 39?	37(5) 39(1,2)	FC	IP	NC	NA
Processing principles	Have you shared the DPO's contact information internally, publicly and with the relevant supervisory authority?	37(7)	FC	IP	NC	NA
	Do you maintain records management and data retention policies?	24(1,2,3)	FC	IP	NC	NA
	Have you documented principles to justify retention periods?	5(1)	FC	IP	NC	NA
	Is personal data processed lawfully, fairly and in a transparent manner?	5(1) 6(1,2,3,4)	FC	IP	NC	NA
	Is personal data collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes?	5(1)	FC	IP	NC	NA
	Is personal data relevant, limited and minimized to what is necessary in relation to the purposes for which they are processed?	5(1)	FC	IP	NC	NA
	Is personal data accurate and kept up to date — and is every reasonable step taken to ensure inaccurate personal data is erased and rectified without delay?	5(1)	FC	IP	NC	NA
	Is personal data kept only for as long as is necessary for the purposes for which it is processed?	5(1)	FC	IP	NC	NA
	Is personal data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures?	5(1)	FC	IP	NC	NA
	Have you clearly identified, detailed, documented and kept up to date the purpose(s) of processing personal data?	5(1)	FC	IP	NC	NA
	Have you implemented appropriate technical or organizational measures to ensure security of personal data, including protection against unauthorized processing, accidental loss, destruction or damage?	5(1) 24(1,2)	FC	IP	NC	NA
	If you process special categories of sensitive data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), are you in compliance with Article 9(2) conditions?	9(1,2)	FC	IP	NC	NA
If you process personal data relating to criminal convictions and offenses or related security measures based on Article 6(1), is this carried out under the control of official authority or authorized by union or member state law?	10	FC	IP	NC	NA	

## 58 «Руководство по выживанию» с GDPR от Linklaters

Processing Condition	Is processing based on the condition contestable?	Does it trigger the 'right to be forgotten'?	Does it trigger the data portability right?	Automated decision making allowed?	Does it trigger additional requirements for privacy notices?	Do you lose the 'one stop shop' mechanism?	Might you be exempt from Privacy Impact Assessments?	Other issues
<b>Consent</b> <i>Art. 6(1)(a)</i>	Yes. Consent can be withdrawn. <i>Art. 7(3)</i>	Yes. Withdrawal can trigger right. <i>Art. 17(1)(b)</i>	Yes. <i>Art. 20(1)(a)</i>	Yes. Explicit consent allows automated decision making. <i>Art. 22(2)(c)</i>	Yes. Must refer to withdrawal right. <i>Art. 13(2)(c)</i> <i>Art. 14(2)(d)</i>	No.	No.	Restrictions on children consenting online. <i>Art. 8</i>
<b>Contract</b> <i>Art. 6(1)(b)</i>	No.	No.	Yes. <i>Art. 20(1)(a)</i>	Yes. Allows automated decision making. <i>Art. 22(2)(a)</i>	No.	No.	No.	No.
<b>Legal obligation</b> <i>Art. 6(1)(c)</i>	No.	No, and may be a defence to the exercise of right. <i>Art. 17(3)(b)</i>	No.	Yes. Allows automated decision making. <i>Art. 22(2)(b)</i>	No.	Yes. <i>Art. 55(2)</i>	Possibly. <i>Art. 35(10)</i>	No.
<b>Vital interests</b> <i>Art. 6(1)(d)</i>	No.	No.	No.	Yes. Individuals have right not to be subject to this. <i>Art. 22</i>	No.	No.	No.	No.
<b>Public functions</b> <i>Art. 6(1)(e)</i>	Yes. Right to object applies. <i>Art. 21(1)</i>	No, and may be a defence to the exercise of right. <i>Art. 17(3)(b)</i>	No. See express exclusion in <i>Art. 20(3)</i>	Yes. Individuals have right not to be subject to this. <i>Art. 22</i>	Yes. Must refer to right to object. <i>Art. 21(4)</i>	Yes. <i>Art. 55(2)</i>	Possibly. <i>Art. 35(10)</i>	No.
<b>Legitimate interests</b> <i>Art. 6(1)(f)</i>	Yes. Right to object applies. <i>Art. 21(1)</i>	Possibly. <i>Art. 17(1)(c)</i>	No.	Yes. Individuals have right not to be subject to this. <i>Art. 22</i>	Yes. Must refer to legitimate interests and right to object. <i>Art. 13(1)(d)</i> <i>14(2)(b) &amp; 21(4)</i>	No.	No.	Cannot be used by public authorities. Can be difficult to use with children. <i>Art. 6(1)(f)</i>

## VISCHER Privacy Score (for the private sector)

Template Version 3.6.2023

English Content

provided by [privacyscore.ch](https://privacyscore.ch)

Questions, feedback, error: [dataprotection@vischer.com](mailto:dataprotection@vischer.com)

Scope: This tool allows you to make a quick overview of the data protection governance, whether the entire company or individual areas and departments. It does not replace the assessment by an expert. You don't check the data protection conformity of individual data processing activities. However, the questionnaire provides information on how well the company has the necessary provisions, responsibilities, regulations and other measures in place to comply with the Swiss Data Protection Act (DPA) and the EU General Data Protection Regulation (GDPR). At the same time, the tool examines which steps can be taken to additionally improve the maturity of the data protection governance. The resulting maturity score (also compared with those of other companies in the sector, including the VISCHER Privacy Score (the only digitalized one) from the VISCHER "Privacy Score" program), are calculated when the answers are recorded in step 3. Please note: All references to the basic DPA refer to the revised Swiss DPA, which will come into force on 1 September 2024. A glossary of terms used can be found at the bottom of the table. About the language: The questionnaires are available in both German and English. You can switch to the top, there will have been no, we will have to create your selection of the scope of the audit, the audit programme and the applicable data protection law. An account always exists, but can be changed or deleted at any time to start with a "fresh" start in another language.

**Step 1: The Organization**

Company: /

Sect. (Race, Country): /

Industry sector (as per NACE): C\_MANUFACTURING

Size of operation: 20-49 (In number of employees, not FTE, the number has no relevance in the calculation of the score or the questions)

Locations, offices: /

---

**Step 2: The Audit Program**

Scope of audit: Single Entity (The scope will impact the available audit program, therefore, if this tool is selected)

Description: / (Data here what you can be in case of scope of your audit)

Inclusions, exclusions: /

Audit program: Detailed Assessment (Privacy Score) (The requirements to step 3 are based on this, therefore, this must be done in detail and should be changed if any)

Data protection law: Swiss DPA-GDPR (The requirements to step 3 are based on this, therefore, this must be done in detail and should be changed if any)

Assessor: /

Date of assessment: /

Contact details: /



The documents you should create, check or obtain:

Privacy Statement (PS); Privacy Policy, governing data protection procedures and responsibilities (PPPR); References to the Privacy Statement on forms, in contracts, in stationary and digital resources (PSR); Records of Processing Activities (ROPA); Records of Processors and DPAs, unless integrated in the Records of Processing Activities (RPO); Data Processing Agreements (DPA); Documents for training employees re data protection and information security (ET); Processing Activity Rulebook (PAR); Concept re User Roles and Privileges (CRP); Emergency Plan (EP); Templates and other resources for assessing and documenting data breaches (TDB); Guidance for employee abroad (GEA); Contractual safeguards for international transfers, such as the EU SCC (SCC); Policy on handling Data Subject Requests (PDSR); Templates and other resources for assessing and documenting Data Subject Requests (TDSR); Records Retention and Deletion Policy (RRDP); Privacy Policy for handling Personal Data (PPRD); Documented Compliance Check of a Processing Activity (CC); Data Protection Impact Assessment (DPIA); Joint Controller Agreement (JCA); Report to the Management on Data Protection Compliance (RMDP); Policy for Employee Monitoring (PEM)

## Step 3: Verification

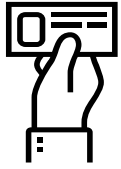
Instructions: Please go through each of the requirements for each of the topics and select the appropriate answer in the "Status" column. If the form has been completed, the appropriate answers have already been entered. A recommendation will automatically be assigned if and what needs to be done to comply with the data protection requirements at how it varies, how best to achieve it about the height of each box. But the answer has to be valid (this has to be done manually). Furthermore, depending on the audit program chosen, the documents required for each requirement are shown in this box. The one summarized along with the corresponding abbreviations. The two columns on the right indicate whether a requirement is relevant or not according to the basis DPA or the GDPR, at the end of each box it is shown how many maturity points (max 3) or risk points (max 1) per requirement the response given by you contributes to the overall score and assessment. Caution: If the subject of the scope, the audit programme or the applicable law or language is subsequently required, the information always recorded will no longer exist.

#	Topic	Requirement	Status	Recommendation	Documents	DPA	GDPR	Maturity points	Risk points
1	Privacy notice	We have a privacy notice (PN)	Yes / Don't know	A PN is mandatory and everyone has to get someone to get an accessible	PN	Must	Must	3	0
2		The PN contains the information required by law	We don't know, but we used a template	Template not fully adapted whether the PN fulfills legal requirements in all relevant aspects	PN	Must	Must	2	2
3		Our PN is translated into every language and can be read in every language in which we normally communicate with our affected persons	We expect that we don't have them in all the languages we communicate in	If the PN is only written in German, it should be available in all the languages of the website if possible, have it translated	PN	Must	Must	3	1
4		We will notify you about the individuals from whom a disclosure can or otherwise collect personal data that we have a PN	The PN is available on the front of our website, but we do not print this out, nor our individuals necessarily own what it is, we are not collecting data about them	The PN is available on the front of our website, but we do not print this out, nor our individuals necessarily own what it is, we are not collecting data about them	PN	Must	Must	3	1
5		If we share personal data about individuals from third party sources (e.g. social media, registers, media or data transfer), we also inform the respective individual of the PN, unless it is in line with a proportionality effect and neither legal obligation apply	The PN is available on the front of our website, but individuals will not own know that it is collecting data about them	The PN is available on the front of our website, but individuals will not own know that it is collecting data about them		Must	Must	3	1

## Records of processing activities и сроки хранения данных

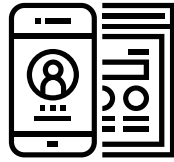


## 61 Источники персональных данных\*



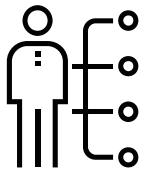
### Предоставленные данные

получены от субъектов или их представителей, например, заполнение веб-форм на сайте, предоставление резюме



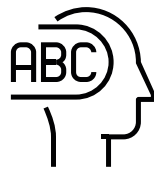
### Распространенные данные

взяты из общедоступных или открытых источников, например, исследование учетных записей в социальных сетях



### Инициированные данные

образованы путем совершения действий в отношении субъектов, например, выплата зарплаты, угон личного автомобиля



### Назначенные данные

временно или постоянно присвоены субъектам, например, номер социального страхования, наименование должности

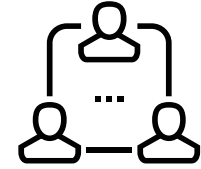
## Behaviour monitoring (GDPR)



Tracking (GDPR)

### Наблюдаемые данные

зафиксированы путем наблюдения за поведением субъектов, например, онлайн-трекинг, геолокация, видеонаблюдение



### Принятые данные

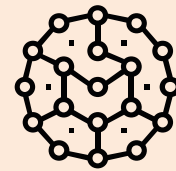
получены не от субъектов или их представителей, а от других лиц, например, рекомендация от бывшего работодателя соискателя



Profiling (GDPR)

### Производные данные

синтезированы после простого анализа других данных, например, расчет прибыльности клиента по количеству посещений и купленных товаров



### Предполагаемые данные

спрогнозированы после продвинутого анализа наборов данных, например, расчет кредитного рейтинга или прогнозирование состояния здоровья

\* - см. Abrams, Martin. The origins of personal data and its implications for governance. OECD, March 2014.

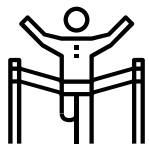
## **CJEU: персональными данными являются как предполагаемые сведения о физическом лице, так и сам источник предположения**

01.08.2022 Суд Европейского Союза ("CJEU") вынес предварительное решение по делу OT v Vyriausioji tarnybinės etikos komisija (Главная комиссия по служебной этике, Литва), согласно **которому специальной категорией персональных данных являются не только носящие предположительных характер чувствительные сведения о физическом лице, но и сведения, которые были использованы для формирования предположения.**

◇ По мнению суда, обработка данных, которые косвенно могут раскрыть чувствительную информацию («специальные категории персональных данных») о физическом лице, не исключается из режима усиленной защиты, т.к. необходимо принять во внимание обработку не только изначально чувствительных данных, но и данных, раскрывающих информацию такого характера косвенно, после интеллектуальной операции, включающей дедукцию (аналитику) или перекрестные ссылки. Например, публикация имени супруга или партнера будет равнозначна обработке специальной категории данных, поскольку она может раскрыть сексуальную ориентацию. И, косвенно, что то же правило применяется к умозаключениям, связанным с другими типами данных специальной категории.

◇ Последствия могут быть еще шире - решение повышает юридический риск для целого ряда других форм онлайн-обработки данных, от приложений для знакомств до отслеживания местоположения и т.д. Так, если человеку понравилась страница Fox News, то это может быть достаточно для вывода о том, что он придерживается правых политических взглядов; или связывание членства в онлайн-группе по изучению Библии с христианскими убеждениями; или покупку детской коляски и кровати, или поход в определенный магазин для вывода о беременности; или вывод о том, что пользователь приложения Grindr является геем или квиром.

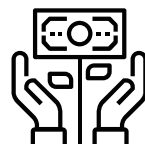
◇ Ранее Федеральный административный суд Австрии своим решением от 26.11.2020 подтвердил позицию Австрийского управления по защите данных ("Datenschutzbehörde") о том, что данные о физическом лице подпадают под понятие "персональные данные", даже если они отражают лишь вероятные, а не фактические характеристики человека.



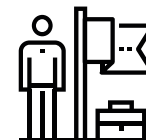
**Подбор  
персонала**



**Управление  
персоналом**



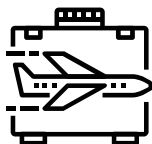
**Вознаграждение  
персонала**



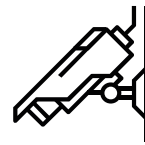
**Обучение и развитие  
персонала**



**Мотивация и  
бенефиты**



**Мобильность и  
релокация**



**Безопасность  
деятельности**



**ИТ-сервисы и защита  
информации**



**Комплаенс и  
делопроизводство**



**Договоры, расчеты и  
закупки**



**Коммуникации,  
маркетинг и продажи**



**Основная  
деятельность**





The screenshot shows the ICO website's navigation and content. The header includes the ICO logo and the text: "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." Below the header is a navigation menu with items: Home, Your data matters, For organisations (selected), Make a complaint, Action we've taken, and About the ICO. The main content area is titled "How do we document our processing activities?" and includes a search bar, a list of related topics, and a detailed section titled "In detail" with several bullet points and sub-sections.

**ico.**  
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters **For organisations** Make a complaint Action we've taken About the ICO

For organisations / Guide to Data Protection / Guide to the General Data Protection Regulation (GDPR) / Documentation /

## How do we document our processing activities?

Share Download options

Search this document

- About this detailed guidance
- What's new under the GDPR?
- What is documentation?
- Who needs to document their processing activities?
- What do we need to document under Article 30 of the GDPR?
- Should we document anything else?
- How do we document our processing activities?**

### In detail

- [How should we prepare?](#)
- [What steps should we take next?](#)
- [How should we document our findings?](#)
- [What should we document first?](#)
- [Is there a template we can use?](#)
- [What if we have an existing documentation method?](#)
- [Do we need to update our record of processing activities?](#)

#### How should we prepare?

A good way to start is by doing an information audit or data-mapping exercise to clarify what personal data your organisation holds and where. It is important that people across your organisation are engaged in the process; this can help ensure nothing is missed when mapping the data your organisation processes. It is equally important to obtain senior management buy-in so that your documentation exercise is supported and well resourced.

#### What steps should we take next?

Once you have a basic idea of what personal data you have and where it is held, you will be in good position to begin documenting the information you must record under the GDPR. It is up to you how you do this, but we think these three steps will help you get there:

## Information Commissioner's Office

Методические рекомендации надзорного органа Великобритании в сфере персональных данных по ведению отчетных записей об обработке персональных данных (Records of Processing Activities) согласно требованию ст.30 GDPR:

для контролеров -

<https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx>

для процессоров -

<https://ico.org.uk/media/for-organisations/documents/2172936/gdpr-documentation-processor-template.xlsx>



The screenshot shows the official website of the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali). The header features the authority's logo and name in Italian. A navigation bar includes links for Home, L'Autorità, Provvedimenti e normativa, Attività e documenti, Stampa e comunicazione, and Attività internazionali. Below the navigation bar, there is a link to a press release from October 8, 2018. The main content area is titled 'FAQ sul registro delle attività di trattamento' and includes a sub-section '1. Cosa è il registro delle attività di trattamento?'. The text explains that Article 30 of the EU Regulation (EU) n. 679/2016 (RGPD) requires the data controller to maintain a register of processing activities. It is described as a document containing key information about processing operations, and it serves as a primary element of accountability for the controller. The register must be in written form, including electronic, and be available for inspection upon request.

**GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

Home L'Autorità Provvedimenti e normativa Attività e documenti Stampa e comunicazione Attività internazionali

VEDI ANCHE: [COMUNICATO STAMPA DELL'8 OTTOBRE 2018](#)

**RGPD**    

## FAQ sul registro delle attività di trattamento

### 1. Cosa è il registro delle attività di trattamento?

L'art. 30 del **Regolamento (EU) n. 679/2016** (di seguito "RGPD") prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del **registro delle attività di trattamento**.

E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento (sul registro del responsabile, vedi, in particolare, il **punto 6**).

**Costituisce uno dei principali elementi di accountability del titolare**, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

## Garante per la protezione dei dati personali

Методические рекомендации надзорного органа Италии в сфере персональных данных по ведению отчетных записей об обработке персональных данных (Records of Processing Activities) согласно требованию ст.30 GDPR.

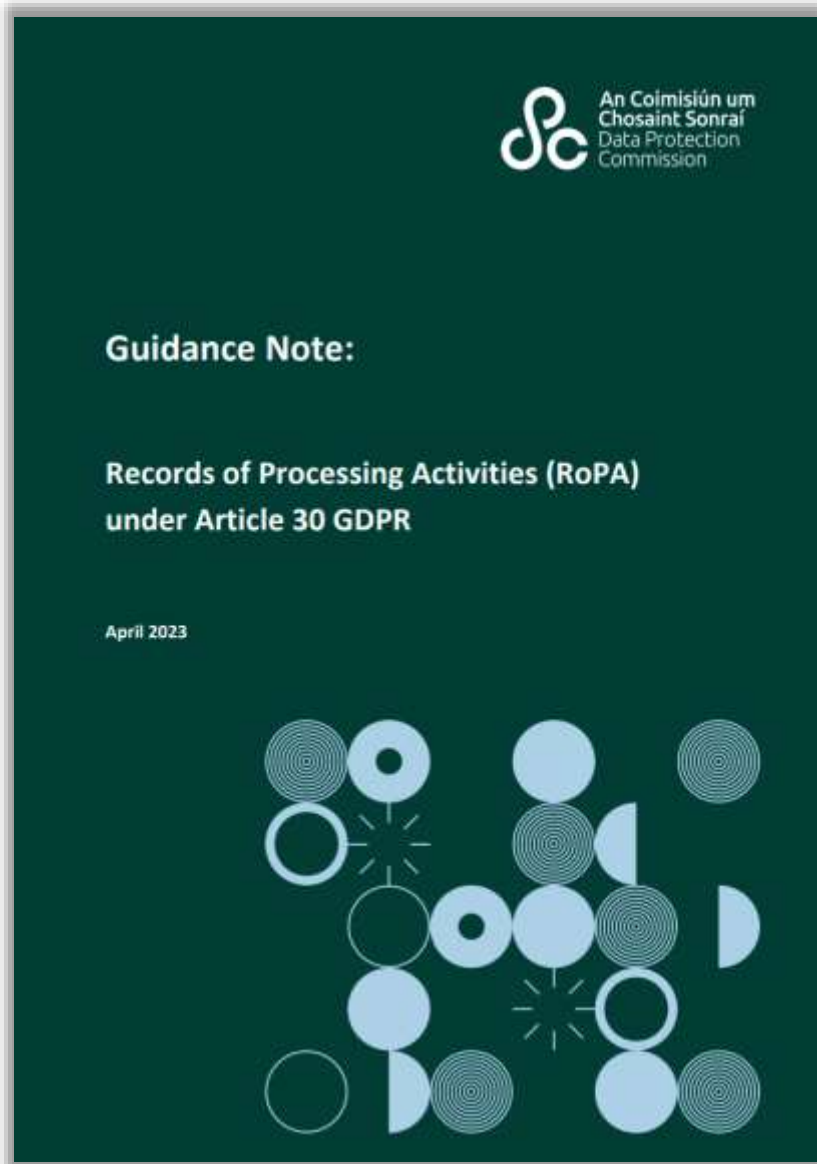
## Рекомендации по учету процессов обработки данных (RoPA) от CNIL

Description of the processing operation							
Name of the processing operation							
N° / REF							
Date of creation of the processing							
Update of the processing							
Stakeholders	Name	Address	ZIP Code	Town	Country	Phone number	Email address
Controller							
Data protection officer							
DPO's Organisation (if external DPO)							
Representative							
Joint controller(s)							
Purpose(s) of the data processing							
Main purpose							
Sub-purpose 1							
Sub-purpose 2							
Sub-purpose 3							
Sub-purpose 4							
Sub-purpose 5							
Category of personal data		Description	Data retention period				
Marital status, ID, identification data, images...							
Personal life (lifestyle, family situation, etc.)							
Economic and financial information (income, financial situation, tax situation, etc.)							
Connection data (IP address, logs, etc.)							
Location data (movements, GSM data, etc.)							
Social Security Number (or NIR)							
Special category of personal data		Description	Data retention period				
Data revealing racial or ethnic origin							
Data revealing political opinions							
Data revealing religious or philosophical beliefs							
Data revealing trade union membership							
Genetic data							
Biometric data for the purpose of uniquely identifying a natural person							
Data concerning health							
Data concerning a natural person's sex life or sexual orientation							
Data relating to criminal convictions and offences							
Category of data subjects		Description	Details				
Category 1		Select an item from the list ►					
Category 2							
Recipients		Type of recipient	Details				
Recipient 1		Select an item from the list ►					
Recipient 2							
Recipient 3							
Recipient 4							
Security measures		Type of security measure	Details				
Security measure 1		Select an item from the list ►					
Security measure 2							
Security measure 3							

## Commission nationale de l'informatique et des libertés

Методические рекомендации надзорного органа Франции в сфере персональных данных по ведению отчетных записей об обработке персональных данных (Records of Processing Activities) согласно требованию ст.30 GDPR.

## Рекомендации по учету процессов обработки данных (RoPA) от DPC



◇ Ирландская Комиссия по защите данных ("DPC") 19.04.2023 опубликовала руководство по ведению записей о деятельности по обработке данных ("RoPA") в соответствии со ст.30 GDPR. RoPA, как мера демонстрации соответствия, является одним из средств, с помощью которых контролеры данных демонстрируют и реализуют принцип подотчетности, изложенный в ст.5(2) GDPR.

◇ В руководстве приводятся примеры надлежащей практики RoPA, например, использование реляционной системы баз данных для группировки деятельности по обработке данных по подразделениям и командам, включая два возможных варианта макета RoPA с использованием программы электронных таблиц, а также примеры рекомендуемых и недостаточно подробных описаний процессов обработки данных.

## Руководство баварского BayLfD по учету процессов обработки данных (RoPA) в государственных органах



Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

### Aktuelle Kurz-Information 47: Frühjahrsputz im Verarbeitungsverzeichnis

**Stichwörter:** Auskunftsrecht, Synergien - Datenschutzbeauftragter, Verarbeitungsverzeichnis - Datenschutzorganisation, Verarbeitungsverzeichnis - Frühjahrsputz, Verarbeitungsverzeichnis - Informationspflichten, Synergien - Verantwortlicher, Verarbeitungsverzeichnis - Verarbeitungsverzeichnis, Aktualisierung | **Stand:** 1. April 2023

#### Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Das Verarbeitungsverzeichnis muss nicht nur angelegt, sondern auch regelmäßig gepflegt werden.
- Jeder Verantwortliche sollte den Geschäftsgang so einrichten, dass er dies gewährleisten kann.
- Was zu tun ist, hängt von den einzelnen Verzeichniseinträgen ab.
- Wer etwas Zeit investiert, trägt dazu bei, dass der Verantwortliche auch bei den Datenschutzhinweisen und im Fall einer Auskunfterteilung "up to date" ist.

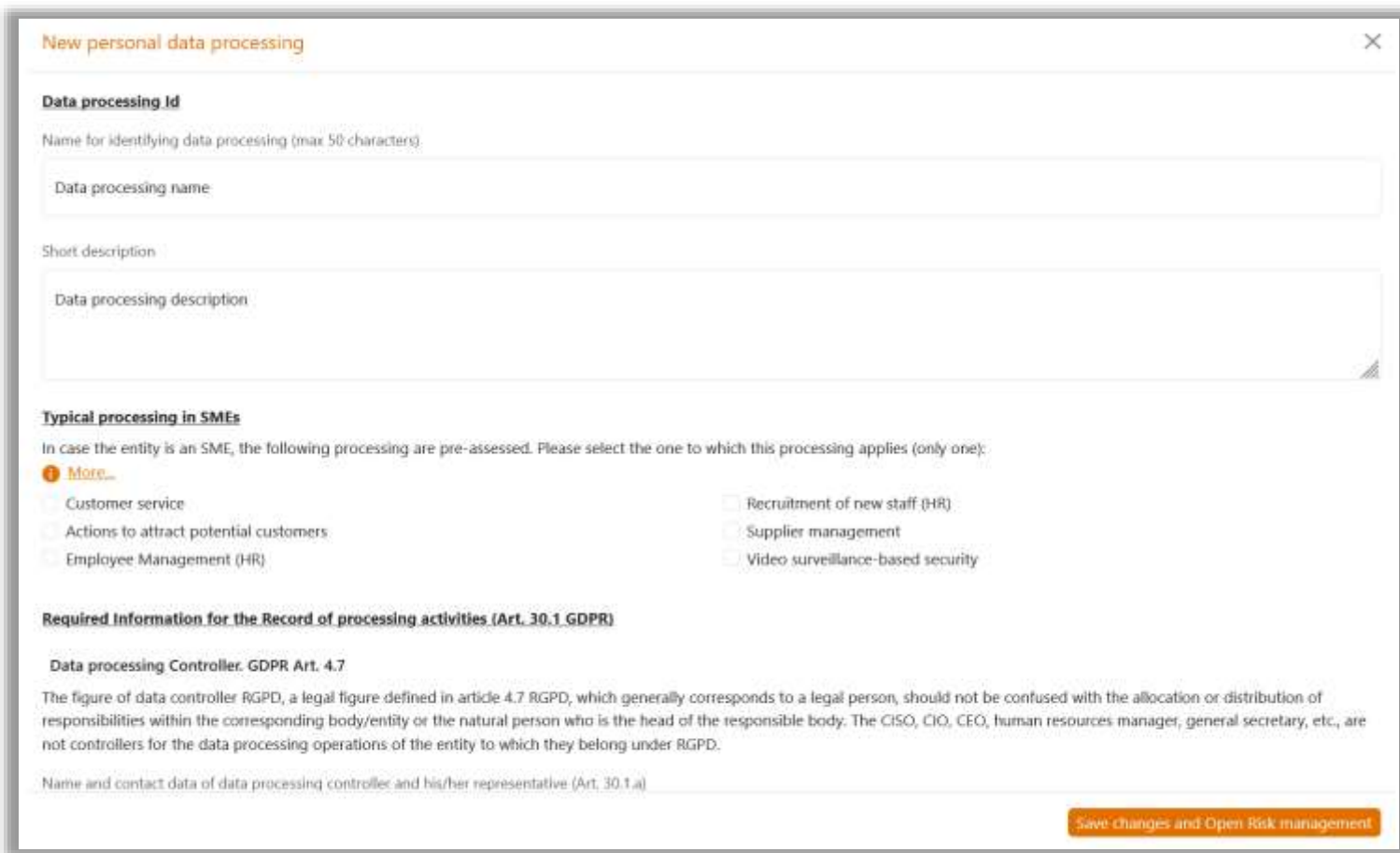
Sie erinnern sich noch, was Sie Anfang 2018 gemacht haben? Sie haben als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter bei einer bayerischen öffentlichen Stelle an der erstmaligen Erstellung des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Datenschutz-Grundverordnung (DSGVO) mitgewirkt? Dann war Ihre öffentliche Stelle damals schneller als viele andere.

Allerdings ist die mühsam erarbeitete Dokumentation nun schon (fast) fünf Jahre alt. Da ist es allerhöchste Zeit, die Texte einmal hervorzuholen, um zu kontrollieren ob noch alles auf dem aktuellen Stand ist. Das sollte nämlich so sein. Das Verzeichnis der Verarbeitungstätigkeiten (im Folgenden kurz: Verarbeitungsverzeichnis) will regelmäßig gepflegt werden. Das vorliegende Papier zeigt auf, worauf dabei zu achten ist. Zur Beruhigung: Man muss meist nicht alles neu machen.

Баварский орган по защите данных ("BayLfD") 01.04.2023 опубликовал руководство по обновлению Реестра записей об обработке персональных данных (RoPA) в государственных органах. В соответствии со ст.30(1)(1) GDPR, ведение и хранение записей об обработке является задачей, относящейся к ответственному за обработку лицу или его представителю, а не к сотруднику по защите данных ("DPO"). Тем не менее, ответственное лицо может делегировать задачи по централизованному администрированию записей об обработке своему DPO, выполняющему консультативные и контрольные функции.

## 70 Веб-сервис «Gestiona» испанского AEPD для ведения RoPA

Веб-сервис предназначен для небольших государственных или частных организаций и позволяет управлять процедурами, осуществлять управление рисками и, при необходимости, оказывать поддержку в проведении оценки воздействия. Инструмент был переработан с более интуитивным дизайном и включает в себя последние рекомендации, содержащиеся в руководствах, опубликованных AEPD. Теперь появляется возможность комплексно вести RoPA организации, включая до 500 видов деятельности по обработке данных, в том числе вести RoPA и проводить DPIA различных организаций.



The screenshot shows a web form titled "New personal data processing" with a close button in the top right corner. The form is divided into several sections:

- Data processing Id:** A section with a label "Name for identifying data processing (max 50 characters)". It contains a text input field labeled "Data processing name" and a larger text area labeled "Short description" with a sub-label "Data processing description".
- Typical processing in SMEs:** A section with a sub-header "Typical processing in SMEs" and a note: "In case the entity is an SME, the following processing are pre-assessed. Please select the one to which this processing applies (only one):". Below this is a "More..." link and a list of six checkboxes:
  - Customer service
  - Actions to attract potential customers
  - Employee Management (HR)
  - Recruitment of new staff (HR)
  - Supplier management
  - Video surveillance-based security
- Required Information for the Record of processing activities (Art. 30.1 GDPR):** A section with a sub-header "Data processing Controller. GDPR Art. 4.7" and explanatory text: "The figure of data controller RGPD, a legal figure defined in article 4.7 RGPD, which generally corresponds to a legal person, should not be confused with the allocation or distribution of responsibilities within the corresponding body/entity or the natural person who is the head of the responsible body. The CISO, CIO, CEO, human resources manager, general secretary, etc., are not controllers for the data processing operations of the entity to which they belong under RGPD." Below this is a text input field labeled "Name and contact data of data processing controller and his/her representative (Art. 30.1.a)".

At the bottom right of the form, there is an orange button labeled "Save changes and Open Risk management".

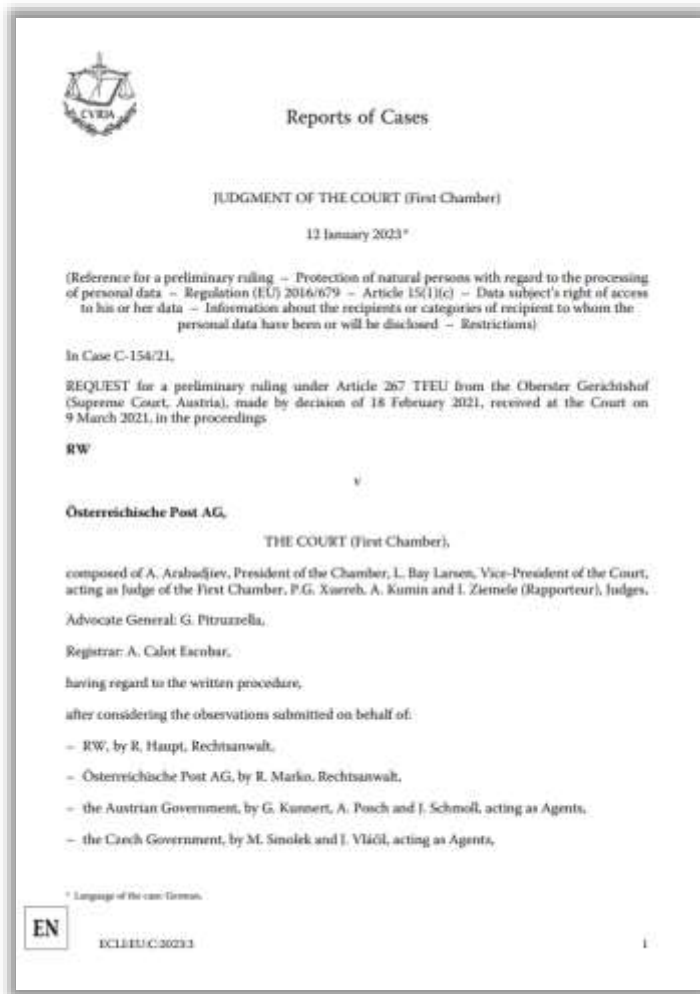
# Рекомендации по учету процессов обработки данных (RoPA) от T4DATA

1. What personal data or categories of personal data are collected and used for this operation?	<i>Tick ✓ as appropriate:</i>	When, how and from whom are the data obtained? E.g.: (data subject=DS) - DWP, upon employing the person - DS, upon enrolment in research
- Given & Family Name(s)		
- Date of Birth		
- Home address		
- Work phone number		
- Private phone number		
- Work email address		
- Private email address		
Add any further data, below if applicable:*		
<i>* See also below, at 2, re sensitive data</i>		
Add further rows if necessary		
2. Do the data you collect and record for the operation <u>include or indirectly reveal</u> any of the following special categories of personal data (“sensitive data”)?	<i>Tick ✓ if the data is expressly collected and used for the operation; Tick ✓ and add (“Indirect”) if the datum is indirectly revealed (explain in a note if necessary)</i>	When and from whom are the data obtained? E.g.: (data subject=DS) - DWP, upon employing the person - DS, upon enrolment in research
- Race or ethnic origin		
- Political opinions or affiliations		
- Religious or philosophical beliefs		
- Trade union membership		
- Genetic data		
- Biometric data		
- Data concerning the		

person's health		
- Data concerning the person's sexual orientation or sex life		
- Information on criminal convictions or offences		
- National identifier* * E.g., NI Number, Tax Number		
- Data about debts/credit score		
- Data on minors		
3. If this is known or determined: How long are the (special and other) data retained? What happens then?*		
<i>* Indicate period or event, e.g., “7 years” or “Until 5 years after termination of employment”. Also explain what happens to the data, e.g., erasure/destruction or rendered anonymous.</i>		
<i>NB: If there are different retention periods for different data, please indicate that.</i>		

## II.2 Disclosures of data

4. To what third parties are which of the above data disclosed? And for what purposes? NB: This also applies to the data being made accessible, especially directly, online Re disclosures involving transfers to third countries, see further below, at II.5	Recipient third party and place and country of establishment:	Purpose(s) of the disclosure(s):
ALL THE DATA LISTED AT II.1		
OR: The following data: (Copy the data from 1 & 2, above)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		



По мнению CJEU, после передачи персональных данных третьим лицам необходимо отслеживать их реальную принадлежность. Простого упоминания "специалиста по маркетингу", "поставщика услуг по расчету заработной платы" или "кадрового агентства" в RoPA под названием "получатели" может быть уже недостаточно.

В RoPA необходимо отслеживать фактическое название/идентификацию компаний или лиц, с которыми персональные данные были переданы или передаются. Таким образом, если субъект данных (например, клиенты, сотрудники и т.д.) спросит вас: "Кому вы передали мои персональные данные и как с ними связаться?", вы сможете предоставить ему обоснованный ответ, а не список общих категорий получателей.

Неполные или неконкретные ответы на запрос субъекта данных в отношении состава получателей персональных данных могут привести к нарушению ст. 5(1)(a), 12 и/или 13(1)(e) GDPR.



## 152-ФЗ



ПП № 1119 / № 687  
и запросы РКН

- работники, обрабатывающие ПД
- цели и основания обработки
- категории ПД и субъектов
- сроки обработки и хранения
- места хранения мат. носителей ПД
- определение угроз безопасности
- перечень мер безопасности мат. носителей ПД

Нет требуемой/рекомендуемой формы ведения  
Реестров – требования только к содержанию документов

## GDPR

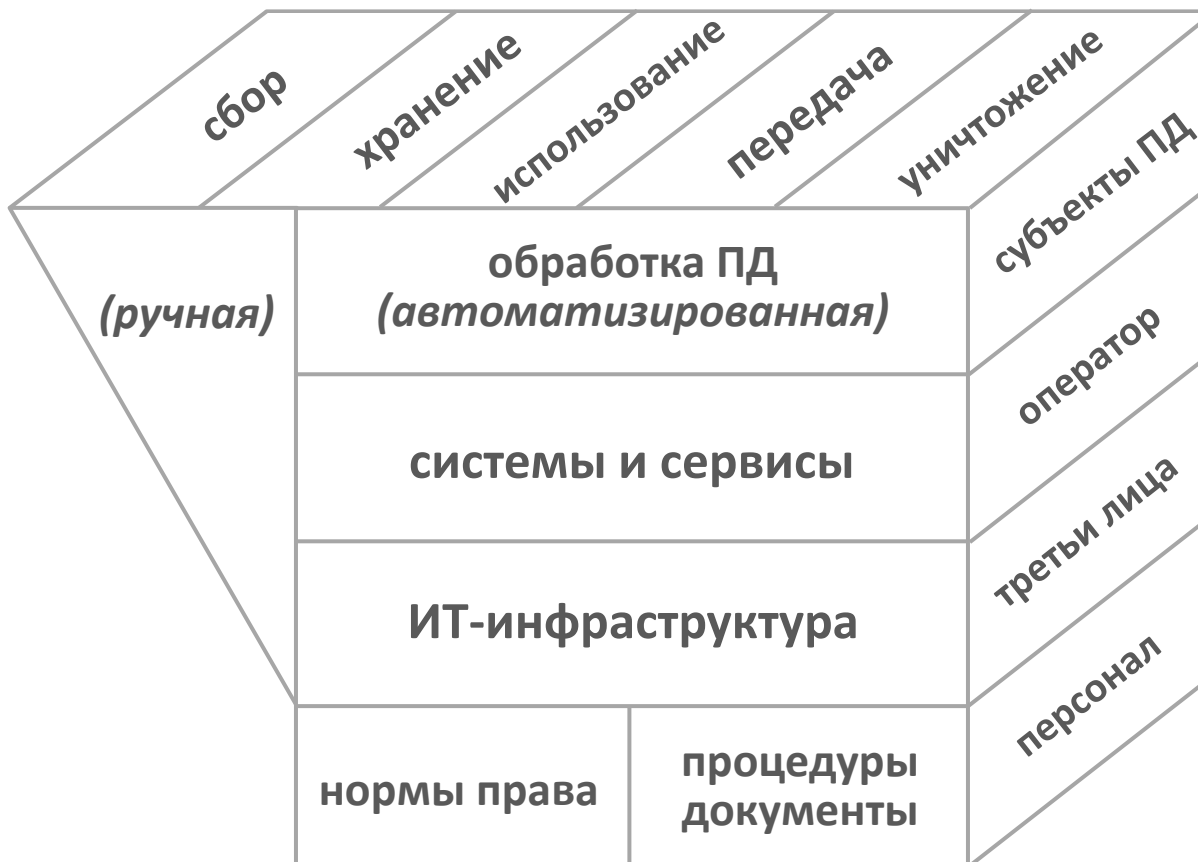


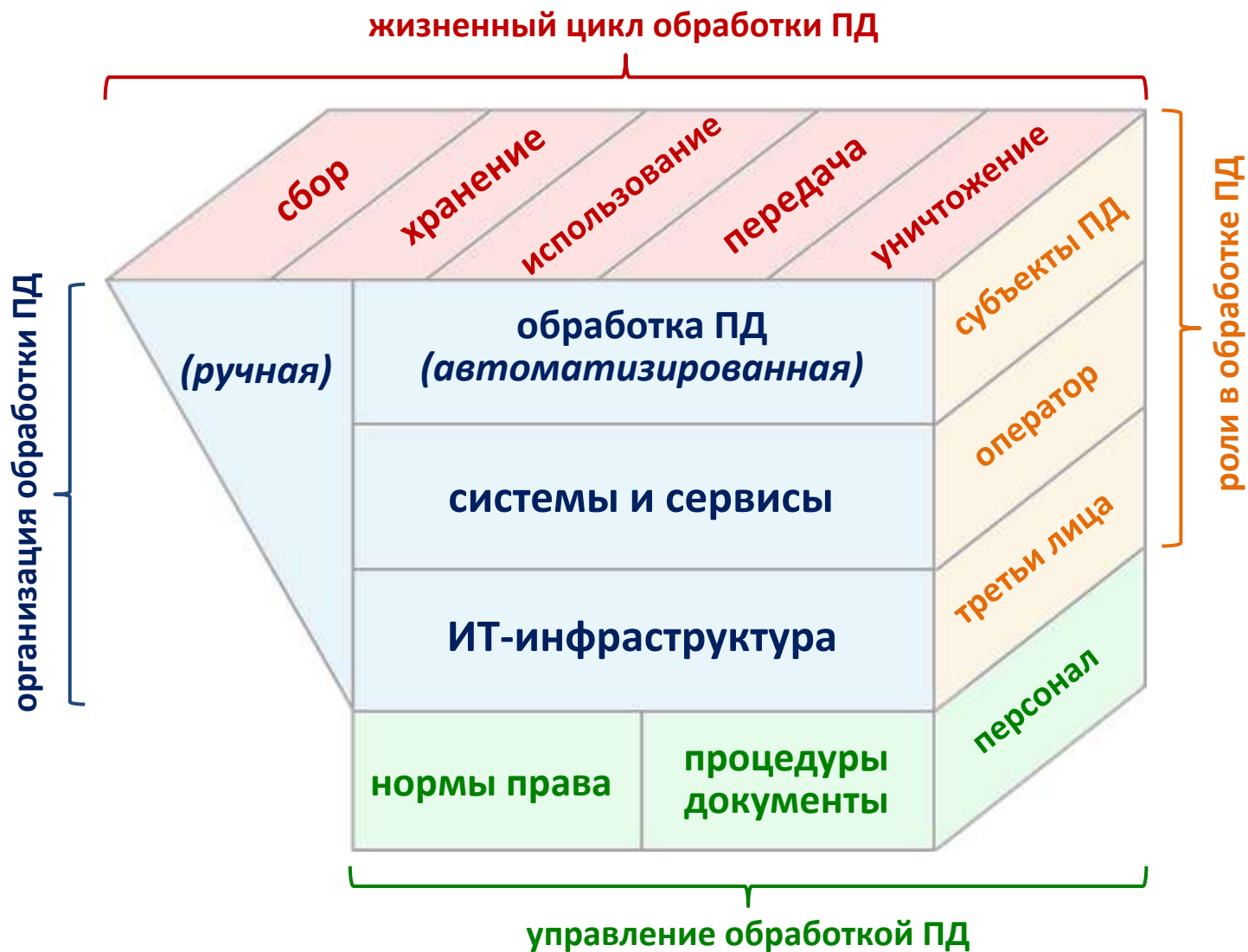
требование  
ст. 30 GDPR

- работники, участвующие в обработке
- цели обработки
- группы субъектов
- обрабатываемые ПД
- срок или условие прекращения обработки
- наименования третьих лиц, которым передаются ПД и страны, наличие договора
- описание мер защиты
- краткое описание процесса
- роль компании
- принадлежность к несовершеннолетним
- основание для обработки
- действия с данными

Рекомендательные формы нац. DPA:  
[EDPS: ICO](#) (Великобритания); [CNIL](#) (Франция);  
[Commissioner for Personal Data Protection](#) (Кипр), др.

[Участники Russian Privacy Professionals Association](#) могут ознакомиться с [материалами семинара виде шаблона RoPA и аналитического перечня платформ по автоматизации ведения RoPA](#) (для получения доступа к материалам необходимо зайти в свою учетную запись на сайте).





## Рекомендации по учету процессов обработки данных (RoPA) для компаний РФ от автора презентации

1.	Обозначение и наименование процесса		
1.1.		<i>Общее описание процесса</i>	
1.1.1.	Домен (макропроцесс)		
1.1.2.	Краткое описание (характер и контекст) процесса		
1.1.3.	Владелец процесса		
1.1.4.	Внутренние участники процесса		
1.1.5.	Перечень локальных актов, регулирующих процесс		
1.1.6.	Источники информации и дата ее предоставления		
1.1.7.	Дата актуальности сведений		
1.2.		<i>Характеристики обработки ПДн</i>	
1.2.1.	Цель обработки ПДн		
1.2.2.	Категории субъектов ПДн		
1.2.3.	Роль <sup>1</sup> Компании в процессе		
1.2.4.	Применимость законодательства <sup>2</sup>		
1.2.5.	Основание обработки ПДн		
1.2.6.	Источник <sup>3</sup> получения ПДн		
1.2.7.	Общие категории ПДн		
1.2.8.	Специальные категории ПДн		
1.2.9.	Биометрические ПДн		
1.2.10.	Геолокационные ПДн		
1.2.11.	Фотоизображения, видео- и аудиозаписи с ПДн		
1.2.12.	Скан-копии и фотокопии документов с ПДн		
1.2.13.	Данные об использовании ИТ-ресурсов и средств связи <sup>4</sup>		
1.2.14.	Действия, совершаемые с ПДн		
1.2.15.	Распространение <sup>5</sup> ПДн		
1.2.16.	Трансграничная <sup>6</sup> передача ПДн		
1.2.17.	Прямые рекламные или информационные контакты		
1.2.18.	Автоматизированное принятие решений		
1.2.19.	Юридически обоснованный срок обработки ПДн		
1.2.20.	Способ <sup>7</sup> обработки ПДн		
1.2.21.	Описание средств автоматизации (ИС) обработки ПДн		
1.2.22.	Местонахождение БД с ПДн и иных серверных компонент		
1.2.23.	Характер подключения средств автоматизации к сетям		
1.2.24.	Типовые формы бумажных носителей ПДн		
1.2.25.	Систематизированные собрания бумажных носителей ПДн		
1.2.26.	Необходимость DPIA и его статус		
1.2.27.	Описание организационных, технических и правовых мер по защите ПДн		
1.2.28.	Примечание		
1.3.		<i>Взаимодействие с третьими лицами при обработке ПДн</i>	
1.3.1.	Наименование <sup>8</sup> третьих лиц		
1.3.2.	Страна(ы) нахождения третьих лиц		
1.3.3.	Описание функционала <sup>9</sup> третьих лиц		
1.3.4.	Основание <sup>10</sup> для взаимодействия с третьими лицами		
1.3.5.	Роль <sup>11</sup> третьих лиц в процессе		
1.3.6.	Характер <sup>12</sup> и способы <sup>13</sup> передачи ПДн		
1.3.7.	Категории ПДн, получаемые и (или) передаваемые		
1.3.8.	Категории ПДн,		
1.3.9.	Действия с ПДн		
1.3.10.	Распространение <sup>14</sup> ПДн		
1.3.11.	Трансграничная передача ПДн		
1.3.12.	Длительность <sup>15</sup> обработки ПДн		
1.3.13.	Способ <sup>16</sup> обработки ПДн		
1.3.14.	Перечень <sup>17</sup> субобработчиков		
1.3.15.	Перечень стран для обработки ПДн		
1.3.16.	Перечень <sup>18</sup> БД (ИС) для обработки ПДн		
1.3.17.	Перечень получателей ПДн		
1.3.18.	Требования к защите ПДн при обработке в ИС		
1.3.19.	Контактные данные <sup>19</sup> третьих лиц		
1.3.20.	Контактные данные <sup>20</sup> представителей третьих лиц		
1.3.21.	Контактные данные <sup>21</sup> DPO третьих лиц		

Типовая форма по ведению отчетных записей об обработке персональных данных (Records of Processing Activities) согласно требованию ст.30 GDPR, которую компании из РФ могут взять за основу для разработки собственной типовой формы. В типовой форме учитываются 110 характеристик в отношении отдельно взятого процесса обработки персональных данных. Форма подготовлена в формате xlsx.

### Sheet n°14: Define a data retention period

11 June 2020

*Personal data cannot be kept for an indefinite period of time: this must be defined according to the purposes of the processing. Once this purpose has been achieved, the data should be archived, deleted or made anonymous (e.g. in order to produce statistics).*

#### Data retention cycles

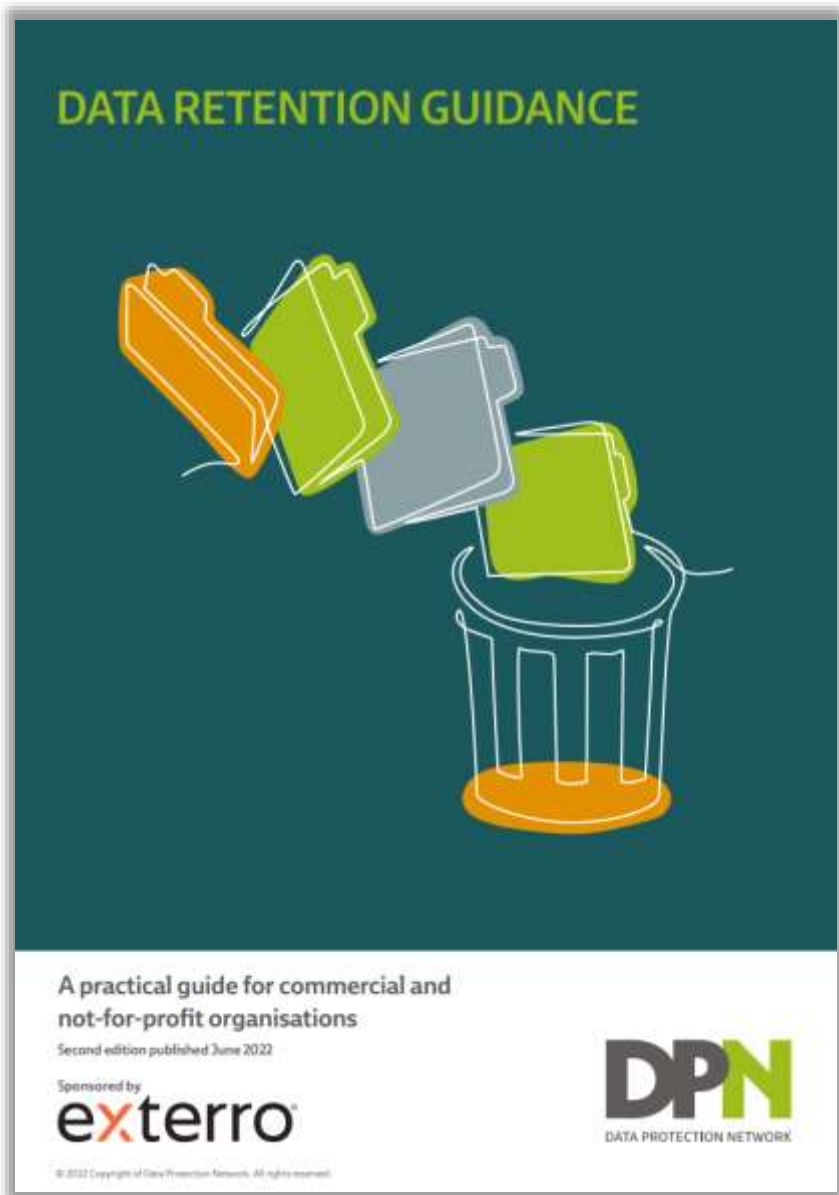
- The personal data retention cycle can be divided into **three distinct successive phases**:
  - The active database;
  - Intermediate archiving;
  - Final archiving or deletion.
- The mechanisms for deleting personal data from the active bases ensure that the data are kept and accessible by the operational services only **for the time necessary to achieve the purpose of the processing operation**.
- Ensure that **data is not kept in active databases** by simply noting them **as being archived**. The archived data (intermediate archive) must be accessible only to a specific service responsible for accessing and removing them from the archive if necessary.
- Please also ensure that you have **specified access modes** for the archived data, as the use of an archive must be on an ad hoc and exceptional basis.
- If possible, use the same implementation when implementing the **data purging or anonymisation** as the one managing the **right to erasure** (see [sheet on the exercise of rights](#)), in order to guarantee a homogeneous operation of your system.

#### Some examples of shelf life

- The **data relating to payroll management or employee time control** can be kept for 5 years.
- The **data in a medical file** must be kept for 20 years.
- The **data of a prospect not responding to any solicitation** can be kept for 3 years.
- The **log data** can be kept for 6 months.

Несколько примеров определения сроков хранения данных:

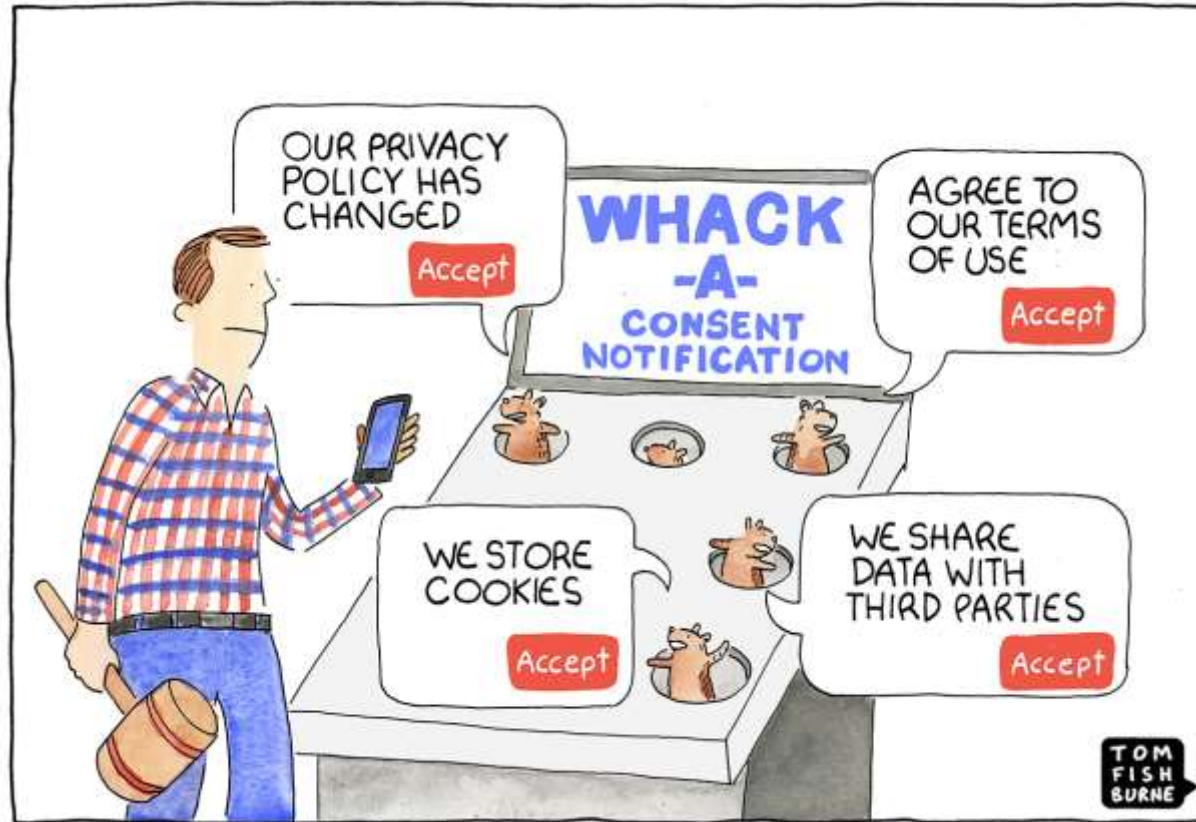
- Данные, касающиеся учета заработной платы или контроля рабочего времени работников, могут храниться в течение 5 лет.
- Данные в медицинской карте должны храниться в течение 20 лет.
- Данные потенциального клиента, не отвечающего ни на какие запросы, могут храниться в течение 3 лет.
- Данные журналирования действий пользователей могут храниться в течение 6 месяцев.

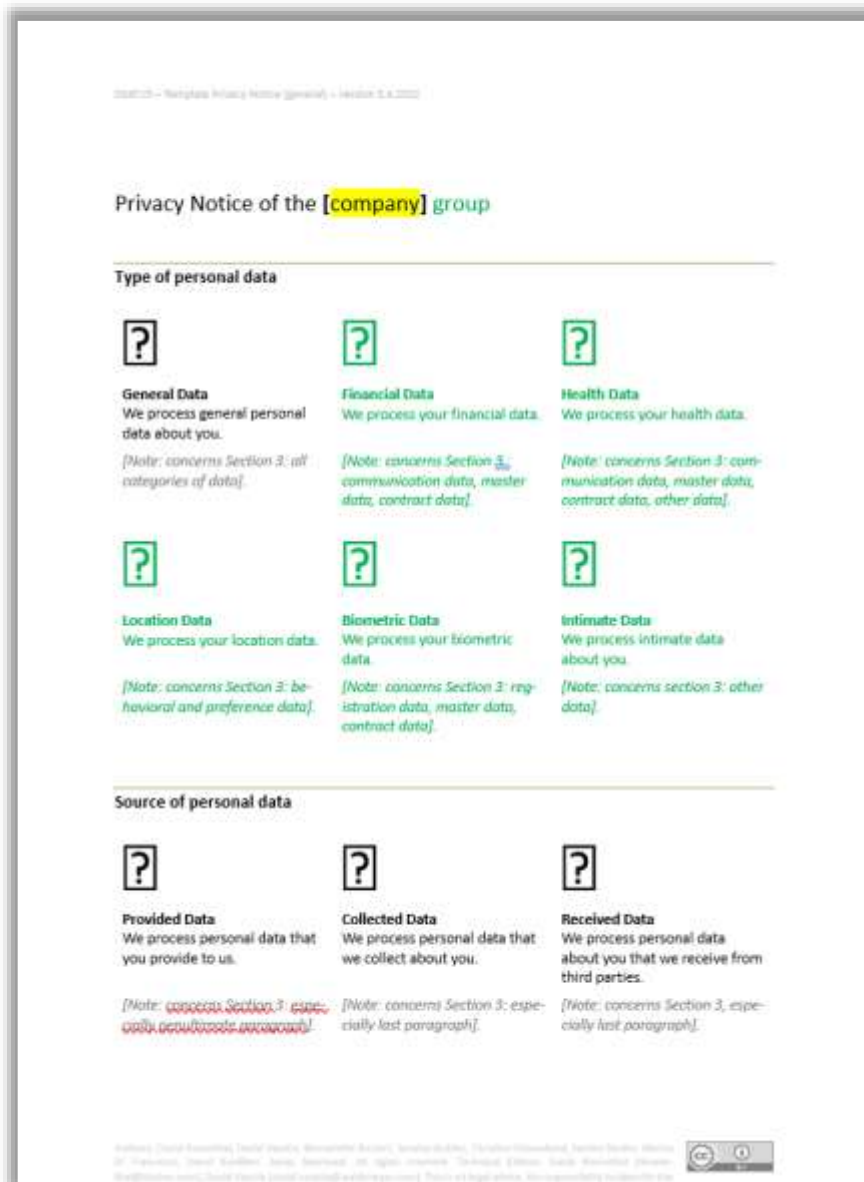
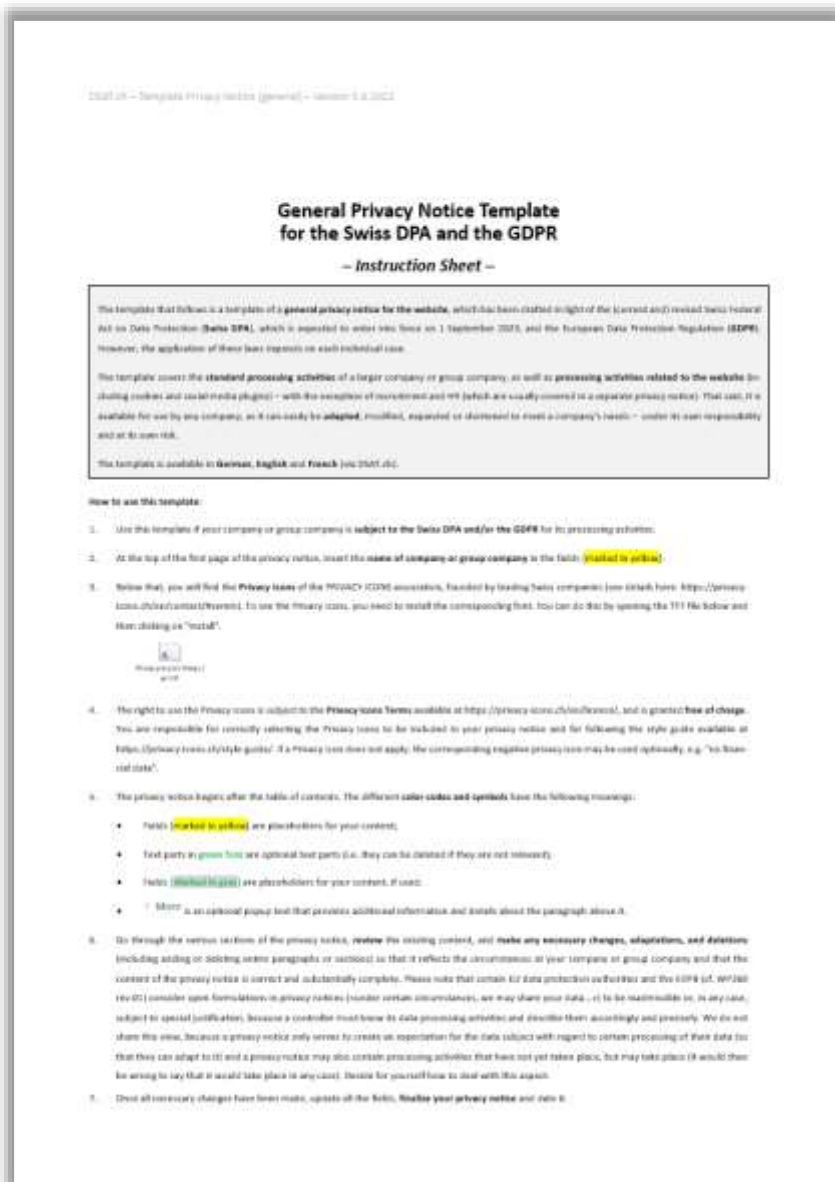


## Data Retention Review Process



## Прозрачность обработки данных и повышение осведомленности







---

## Readability Test

---

You are here: [Home](#) → [Quality Assurance](#) → **Readability Test**

---

→ [Site Navigation](#)

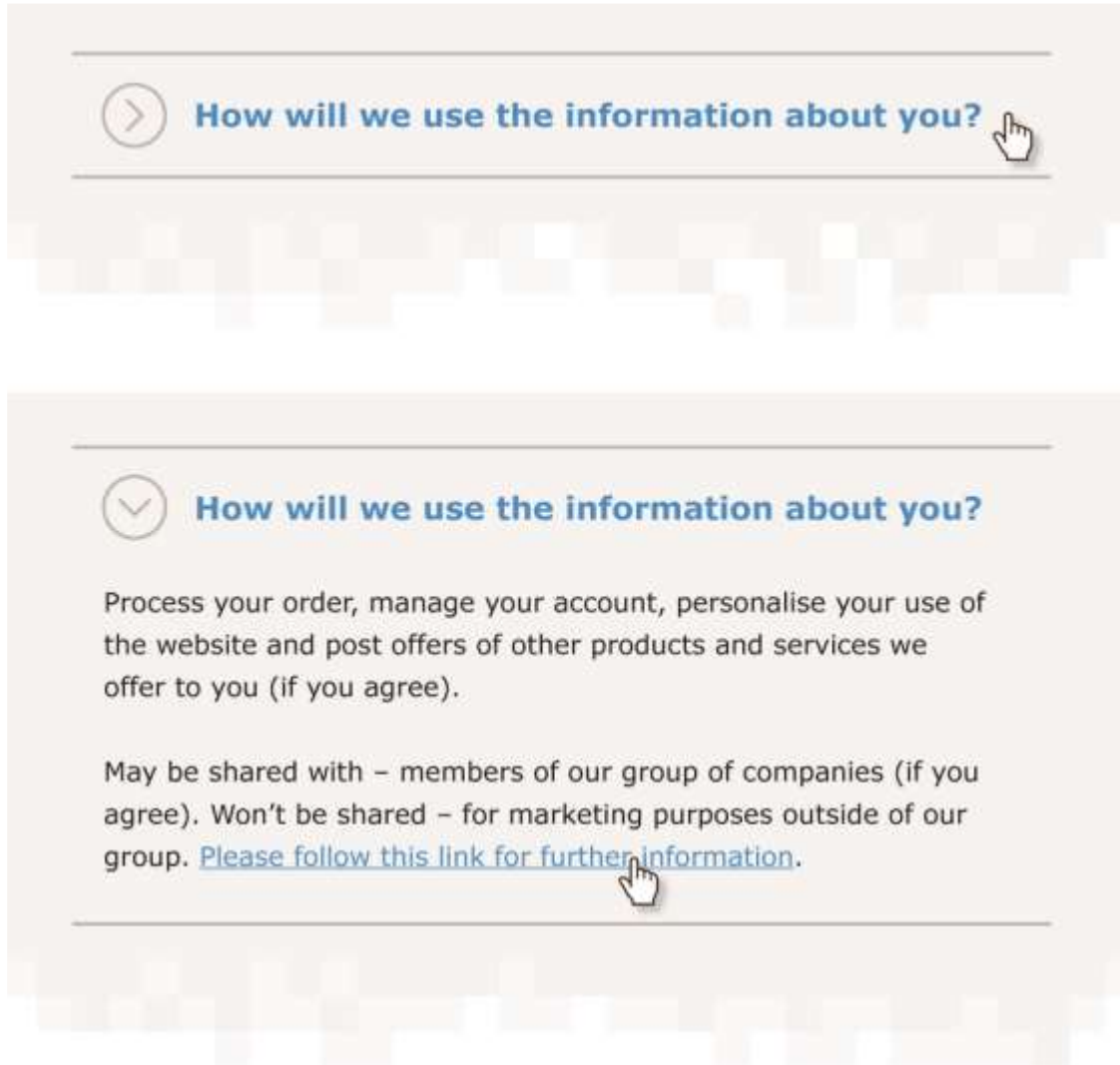
### Contents

- [Readability Tests](#)
- [Test the Readability of a Website](#)
- [Interpreting the Results](#)
- [Gunning-Fog Index](#)
- [Flesch Reading Ease](#)
- [Flesch-Kincaid grade level](#)
- [Reading Level Algorithms](#)
- [Further Reading](#)

### Readability Tests

Gunning Fog, Flesch Reading Ease, and Flesch-Kincaid are [reading level algorithms](#) that can be helpful in determining how readable your content is. Reading level algorithms only provide a rough guide, as they tend to reward short sentences made up of short words. Whilst they're rough guides, they can give a useful indication as to whether you've pitched your content at the right level for your intended audience.

## 82 Многоуровневые документы (layered documents)



## 83 Своевременные уведомления (just-in-time notice)

### Create an account

Title

Mr

Name

Joe Bloggs

Email address



Username

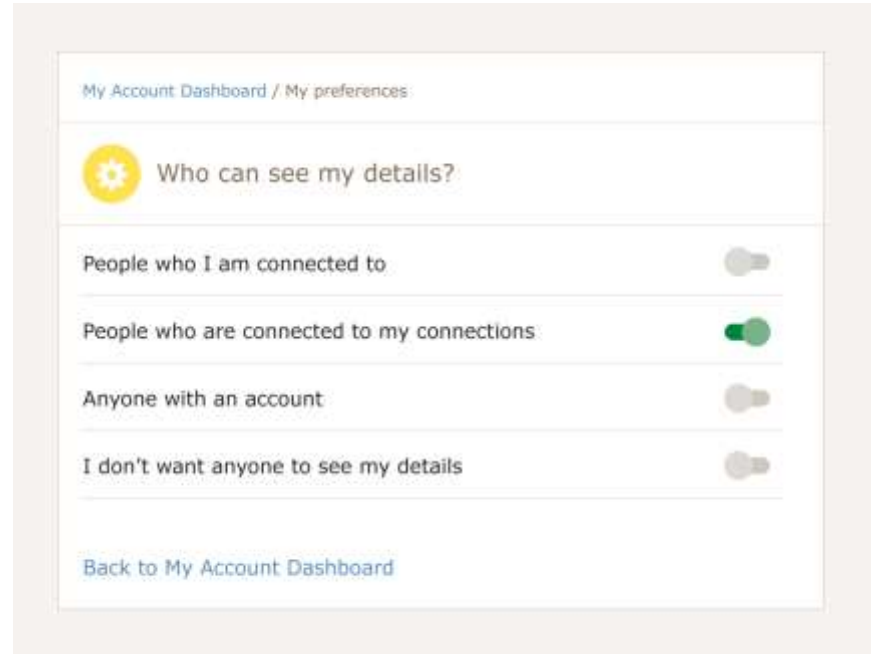
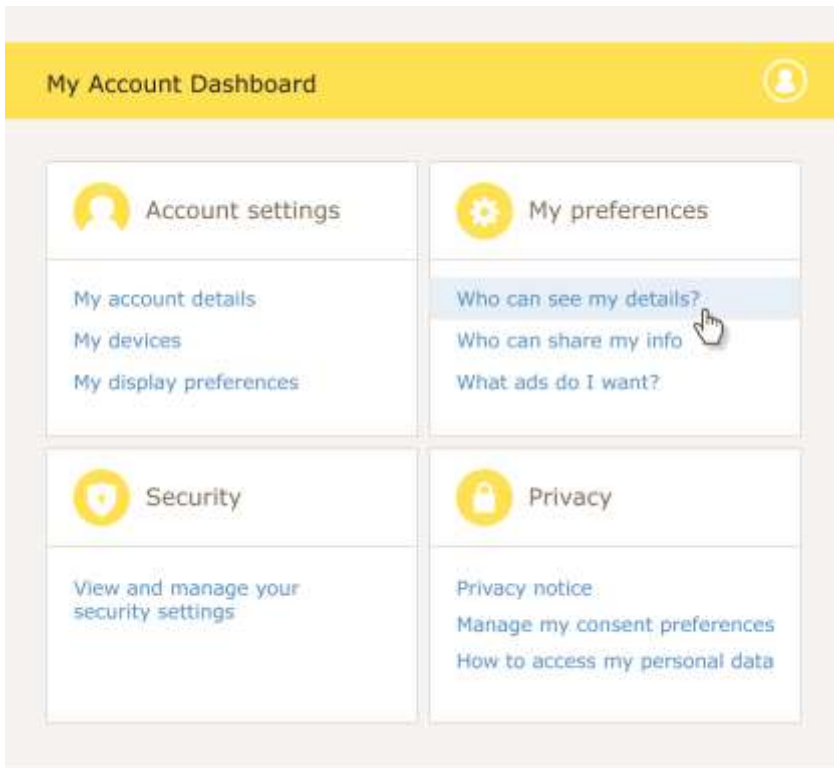
Password

Confirm password

Create account

We use your email address as part of allowing you access to your account, and in order to contact you with important information about any changes to your account. [Please follow this link for further information.](#)

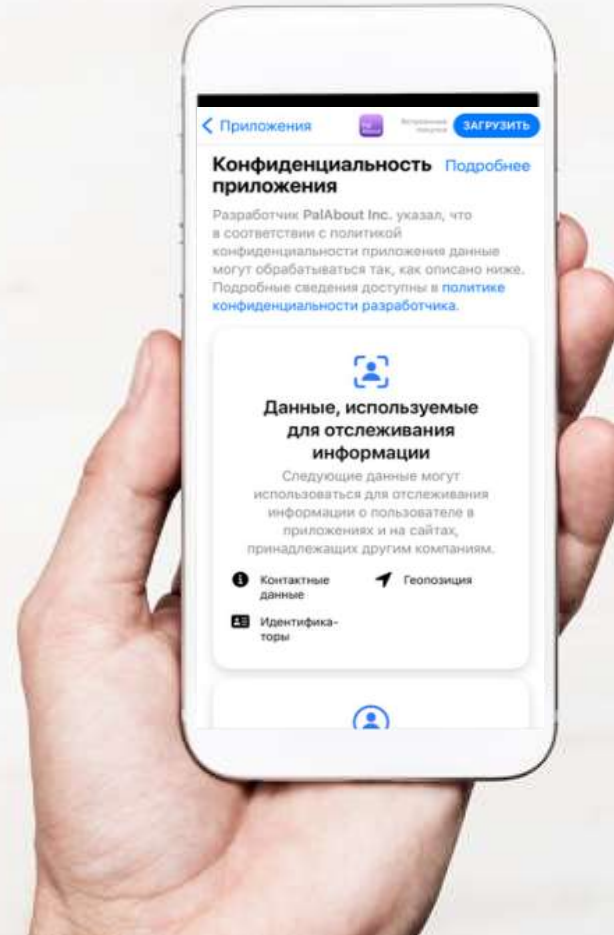
## 84 Панели управления приватностью (privacy dashboard)



App privacy labels  
App privacy details  
Describing Data Usage  
Privacy information

«Этикетка с составом» для приложения, связанная со сбором данных: ярлык показывает, какие данные собираются приложением и для какой цели

Eric Benjamin Seufert



## 86 Наборы информационных иконок по приватности от итальянского Garante



L'interessato



Dati personali dell'interessato



Il titolare del trattamento



Il contitolare del trattamento



Il rappresentante



Il responsabile della protezione dati



Il responsabile del trattamento dati



L'autorità di controllo



Dati del titolare del trattamento



Dati del contitolare del trattamento



Dati del rappresentante



Dati del responsabile della protezione dati



Dati del responsabile del trattamento dati



Finalità del trattamento



Base giuridica del trattamento



Legittimi interessi perseguiti dal titolare



Destinatari dei dati personali



Trasferimento dei dati



Periodo di conservazione dei dati



Diritti dell'interessato

# 87    **Sammlungen von Informations-Symbolen zur Privatsphäre von LfDI Baden-Württemberg**

## 1. Verantwortliche\_r



## 2. Personenbezogene Daten



## 3. Zweck



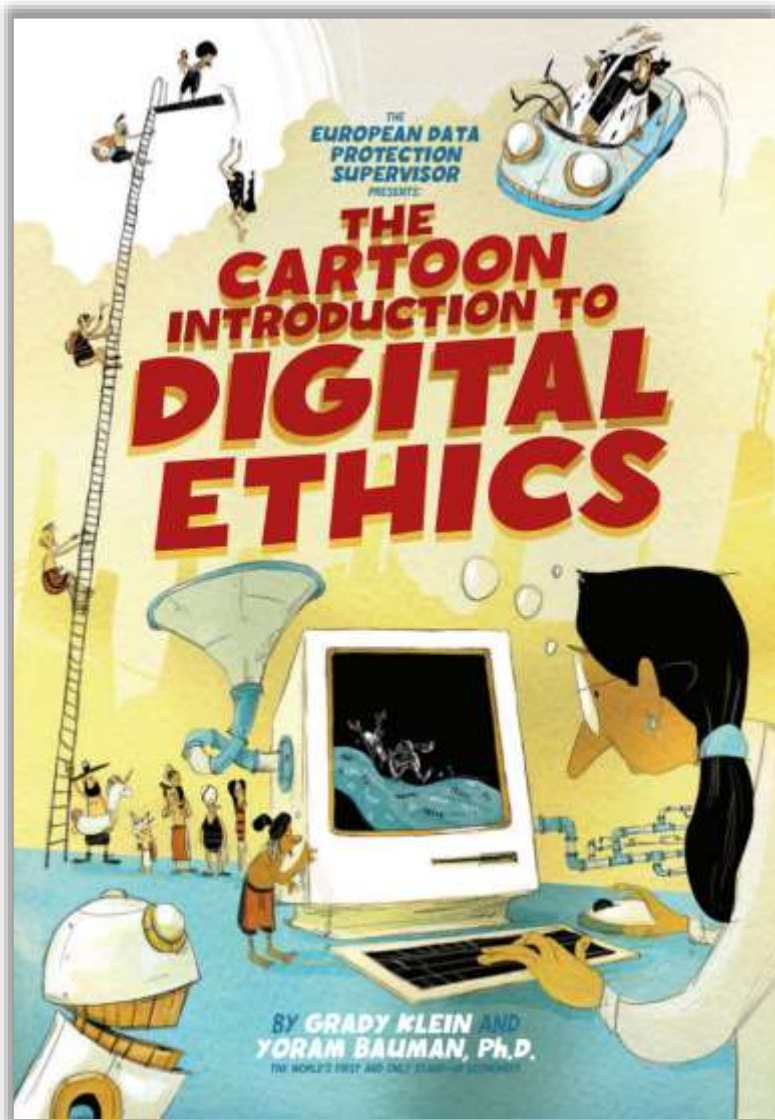
## 4. Rechtsgrundlage



## 5. Betroffenenrechte



88 Комиксы от Европейского надзорного органа по защите данных





## 89 База с «тёмными» паттернами

Тёмный паттерн (англ. **dark patterns**) — это пользовательский интерфейс, который заставляет вас делать то, чего обычно вы бы не сделали. Например, подписаться на рассылку, купить премиум-версию программы вместо пробной или нажать на уведомление.

Please enter your details to reserve your item(s)

Title :

First name \* :

Last name \* :

Email \* :

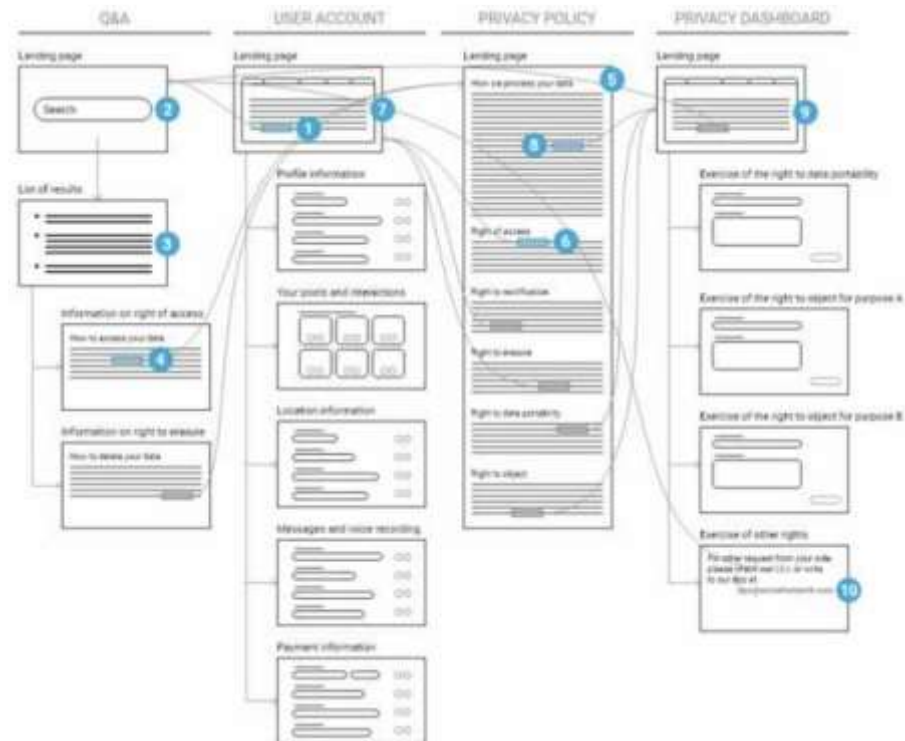
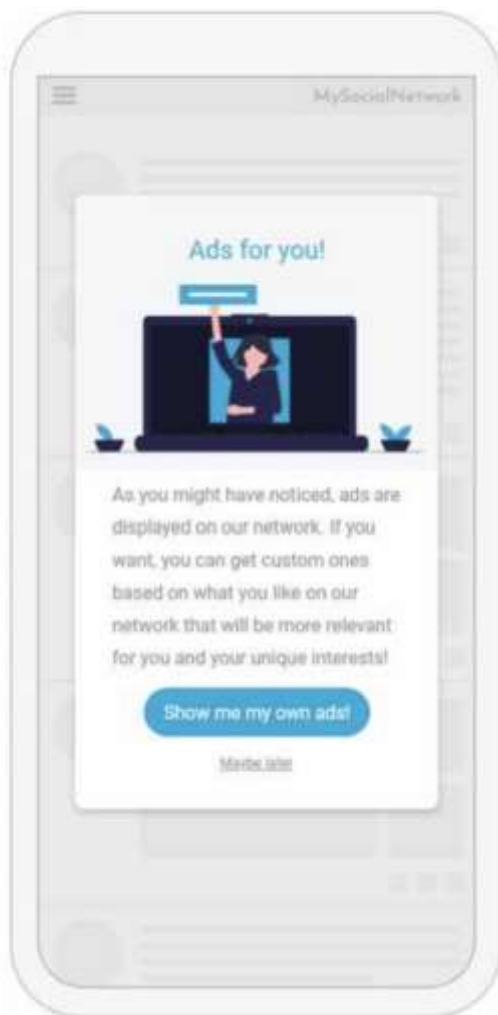
Phone number \* :

Please do not send me details of products and offers from Currys.co.uk

Please send me details of products and offers from third party organisations recommended by Currys.co.uk

## Руководство EDPB по «тёмными» паттернам в интерфейсах социальных сетей: как их распознать и избежать

Timeline of the user interactions where the pop-up is displayed





### Modelli di progettazione ingannevoli (Dark Pattern)

### Modelli di progettazione ingannevoli (Dark Pattern)

Con la definizione di "modelli di progettazione ingannevoli" vengono indicate quelle interfacce e quei percorsi di navigazione progettati per influenzare l'utente affinché intraprenda azioni inconsapevoli o non desiderate - e potenzialmente dannose dal punto della privacy del singolo - ma favorevoli all'interesse della piattaforma o del gestore del servizio.

Detti anche **Dark Pattern**, i modelli di progettazione ingannevoli mirano dunque a influenzare il nostro comportamento e possono ostacolare la capacità di proteggere efficacemente i nostri dati personali.

Il 24 febbraio 2023, il [Comitato europeo per la protezione dati \(EDPB\)](#) ha pubblicato le [linee guida](#) su come riconoscere ed evitare questi sistemi. Il documento offre raccomandazioni pratiche a gestori dei social media, a designer e utenti su come comportarsi di fronte a queste interfacce che si pongono in violazione del Regolamento europeo in materia di protezione dati.

Le linee guida dell'EDPB individuano sei tipologie riguardo alle quali si può parlare di "modelli di progettazione ingannevoli":

- quando gli utenti si trovano di fronte a una enorme numero di richieste, informazioni, opzioni o possibilità finalizzate a spingerli a condividere più dati possibili e consentire involontariamente il trattamento dei dati personali contro le aspettative dell'interessato (*overloading*)
- quando le interfacce sono realizzate in modo tale che gli utenti dimentichino o non riflettano su aspetti legati alla protezione dei propri dati (*skipping*)
- quando le scelte degli utenti sono influenzate facendo appello alle loro emozioni o usando sollecitazioni visive (*stirring*)
- quando gli utenti sono ostacolati o bloccati nel processo di informazione sull'uso dei propri dati o nella gestione dei propri dati (*hindering*)
- quando gli utenti acconsentono al trattamento dei propri dati senza capire quali siano le finalità a causa di un'interfaccia incoerente o poco chiara (*wickie*)
- quando l'interfaccia è progettata in modo da nascondere le informazioni e gli strumenti di controllo della privacy agli utenti (*leftinthedark*)

Ricordiamo che interfacce e informazioni sottoposte agli utenti dovrebbero sempre riflettere fedelmente le conseguenze dell'azione intrapresa ed essere coerenti con il percorso di esperienza-utente.

L'approccio alla progettazione deve essere dunque quello di non mettere in discussione la decisione della persona per indurla a scegliere o mantenere un ambiente meno protettivo nei

Italiano орган по защите данных ("Garante") 20.04.2023 запустил на своем сайте информационный ресурс о темных паттернах ('dark patterns'). Интерфейсы и информация, предоставляемая пользователям, всегда должны точно отражать последствия предпринятых ими действий и соответствовать пользовательскому опыту. Необходимо использовать добросовестный подход к проектированию пользовательских интерфейсов, чтобы пользователи осознавали риск своих действий в отношении собственных данных и конфиденциальности.

## 92 Руководство британских ICO и CMA о вредном дизайне веб-сайтов



09.08.2023 исполнительный директор Управления комиссара по информации (ICO) по регуляторным рискам опубликовал совместное сообщение со старшим директором отдела цифровых рынков Управления по конкуренции и рынкам (CMA), в котором объявил о выпуске совместного документа ICO-CMA о вредном дизайне на цифровых рынках. Документ адресован веб-дизайнерам, разработчикам и организациям, создающим веб-сайты.

В частности, использование в веб-дизайне формулировок, предполагающих правильное или неправильное решение в отношении политики конфиденциальности или упрощение определенных вариантов, чтобы склонить пользователя к выбору того или иного варианта, может нарушать законодательство о защите данных. Кроме того, такие методы дизайна вызывают опасения с точки зрения потребительского и антимонопольного законодательства.



Голландское управление по защите данных (AP) 05.12.2023 выпустило руководство для крупных компаний, призвав их повысить прозрачность своей практики защиты конфиденциальности. Вопросы конфиденциальности должны быть увязаны с корпоративной социальной ответственностью, поскольку компании все больше внимания уделяют устойчивому развитию и этическим соображениям. Кроме того, признавая растущее использование данных на фоне цифровизации и требований GDPR, AP призвал компании активно сообщать о том, как они устраняют риски, связанные с конфиденциальностью, чтобы укрепить доверие клиентов, сотрудников и акционеров.

Было опубликовано:

- руководство по включению информации о конфиденциальности в годовые отчеты;
- руководство по роли наблюдательных советов в организации и управлении рисками конфиденциальности в компаниях.

## Отчет американской FTC по «тёмными» паттернам в пользовательских интерфейсах

The screenshot shows a loan agreement page from Lending Club. The page is titled "Lending Club" and "Loan Rate & Terms". It contains various sections including "Loan Summary", "Loan Details", "Late Charges", "Prepayment Policy", and "Other than payment dates, items marked (e) will decrease if you receive less than 100% funding." The page is cluttered with text and small fonts, making it difficult to read. A blue callout box highlights a specific section of the text.

Late charges: If your payment arrives after your 15 day grace period, you will be charged a late fee equal to the greater of: 5.00% of the late payment amount or \$15. This fee is charged only once per late payment.

Prepayment policy: If you pay off your loan early, you will not be charged a penalty. In the event of a full prepayment, you may be entitled to a refund of part of the finance charge.

See your borrower agreement for any additional information about nonpayment, default, or other matters related to your loan.

(e) means estimate

Other than payment dates, items marked (e) will decrease if you receive less than 100% funding. Regardless of the ultimate amount of the loan, your APR will not change. Subject to your right to cancel, an unsecured loan may issue for less than the full requested loan amount if it is not 100% funded by the end of the listing period.

Total Amount Requested: \$10,000.00  
Origination Fees: \$500.00  
Total Amount Received: \$9,500.00

Unsuccessful payment fee. When a payment fails and is rejected by your bank, you will be charged an Unsuccessful Payment Fee of \$15 to cover the cost Lending Club incurs on the transaction. Each attempt to collect a monthly payment is considered a separate transaction, so an Unsuccessful Payment Fee will be assessed for each failed attempt.

Федеральная торговая комиссия США (FTC) выпустила отчёт по тёмным паттернам — это методы проектирования пользовательских интерфейсов, которые используются в попытке склонить пользователя к действиям, которые он считает нежелательными.

Как пример — непримечательная галочка в форме, которая приводит к покупке ненужной дополнительной услуги или передаче пользовательских данных. Намеренно спрятанная за десятью кликами кнопка отписки от сервиса тоже является тёмным паттерном.

В общем, запутать пользователя и повысить конверсию/понижить отток стремятся все, а в FTC предприняли попытку придать все эти трюки таксономии и регуляции, оставив чёткий посыл всем growth-хакерам — «we will continue to take action».

## Информационный плакат о работе с персональными данными в печатных документах от датского Datatilsynet

# Pas på data – også på print

**1 Når du printer: Personoplysninger skal udskrives sikkert – derfor er det vigtigt:**

- At du – hvis du kan – bruger 'follow me' / 'skyprint' e.l., hvor det kun er dig, der kan hente dit eget print.
- At du tager dine dokumenter med, så de ikke ligger og flyder i printerrummet.
- At rydde op i printerrummet jævnligt.

**2 Når du tager materialet med dig: Fysisk materiale med personoplysninger skal opbevares og transporteres sikkert. Husk:**

- At holde øje med materialet under transport.
- Sikker opbevaring af fortroligt materiale, der ikke er under opsyn – lås det indel.
- Ikke at opbevare materialet sammen med værdigenstande – det kan øge risikoen for tyveri.

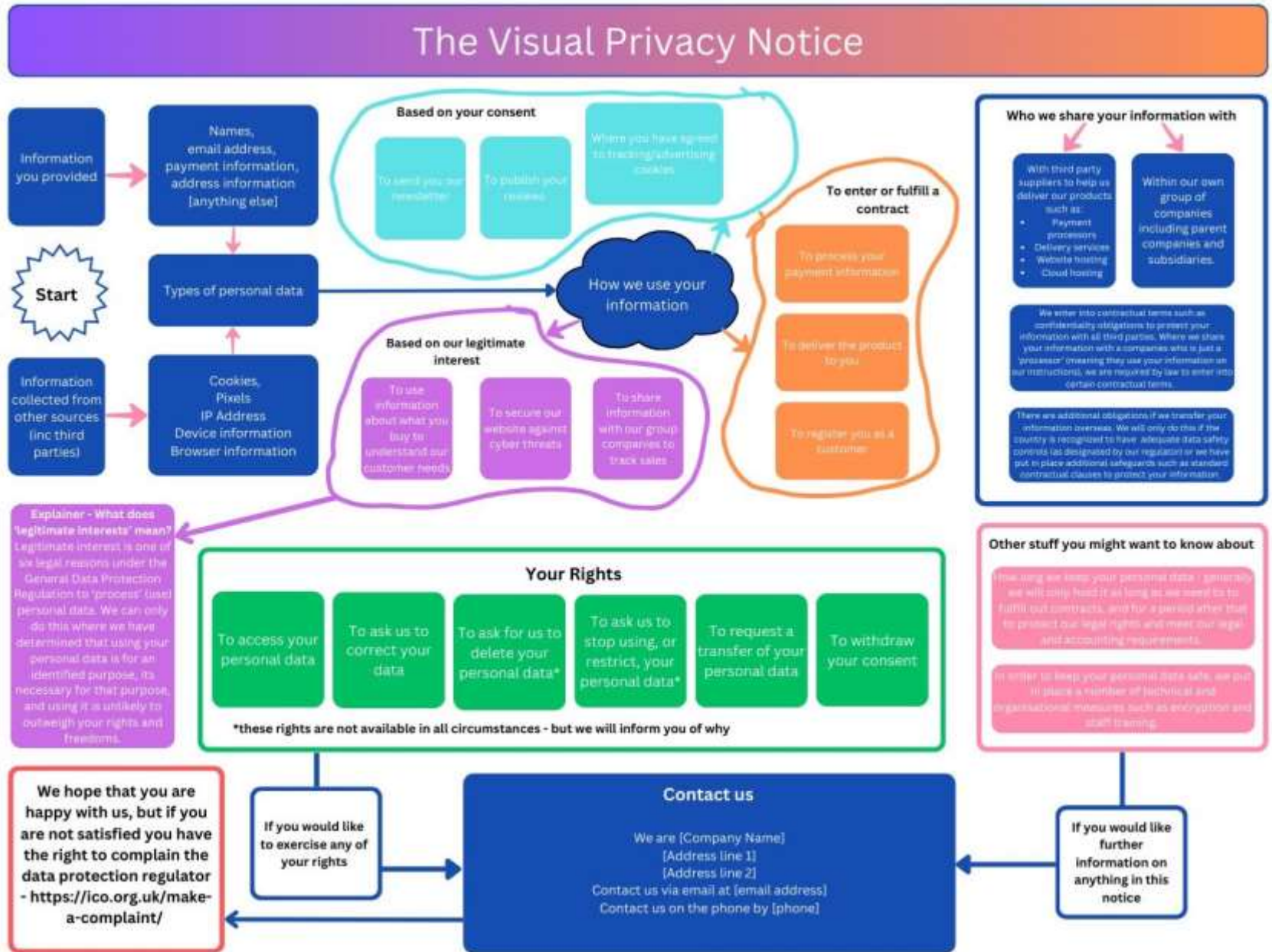
**3 Når du er færdig med materialet: Håndter materialet korrekt, når du ikke længere skal bruge det. Derfor skal du:**

- Selv makulere materialet med det samme – eller lægge det i fx aflåste containere, hvor det løbende bliver hentet og destrueret.



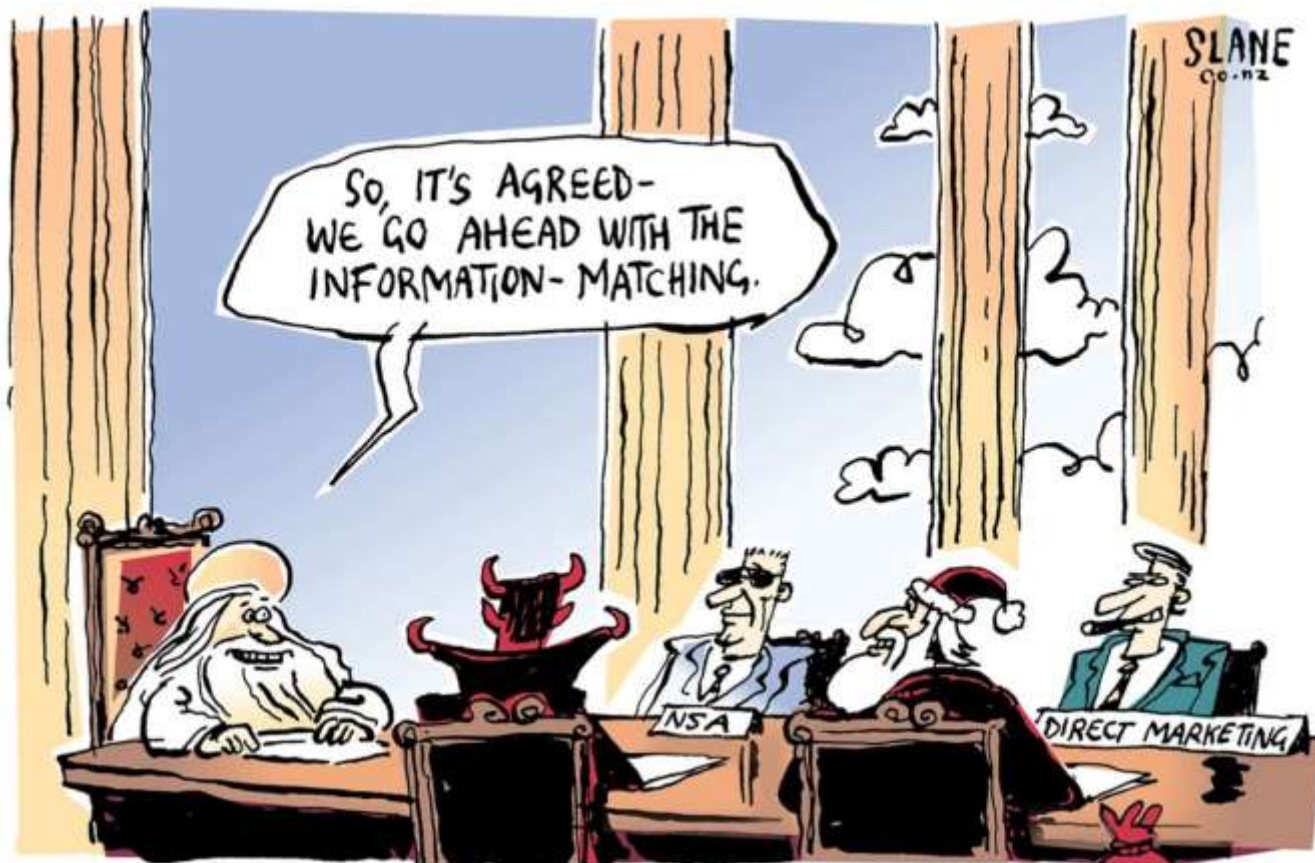
Датский орган по защите данных ("Datatilsynet") опубликовал 20.12.2022 информационный плакат, содержащий советы по безопасной обработке персональных данных в печатных документах. Печатные персональные данные также подпадают под действие GDPR, и что, соответственно, плакат, который можно повесить в типографиях, может помочь организациям обеспечить безопасность печатных персональных данных.

96 Пример визуализации уведомления о конфиденциальности (Privacy notice)





## Processing grounds and Legitimate Interests Assessment





## The EDPS quick-guide to necessity and proportionality



Processing of personal data - be it collection, storage, use or disclosure - **constitutes a limitation** on the right to the protection of personal data and must comply with EU law. This requires ensuring that it is both **necessary and proportional**.

The **8 steps** outlined below will help you assess the compatibility of measures impacting the fundamental rights to privacy and to the protection of personal data with the **EU Charter of Fundamental Rights**.

They are based on the EDPS [Necessity Toolkit](#) and [Guidelines on Proportionality](#).

In case of questions, please contact the EDPS Policy and Consultation Unit  
POLICY-CONSULT@edps.europa.eu

[www.edps.europa.eu](http://www.edps.europa.eu)

@EU\_EDPS

EDPS

European Data Protection Supervisor



### Assessing necessity:

**1** **Factual description** of the measure.

**2** **Identify fundamental rights and freedoms** limited by data processing. Is there a limitation of the rights to privacy and to the protection of personal data, and possibly also of other rights?

(\* In any case, the measure must respect the essence of the rights.)

**3** **Define the objectives** of the measure. These may include an objective of general interest recognised by the Union or the need to protect the rights and freedoms of others.

**4** Choose **the option that is effective and least intrusive**. The measure should be genuinely effective and the least intrusive for the rights at stake.

### Assessing proportionality:

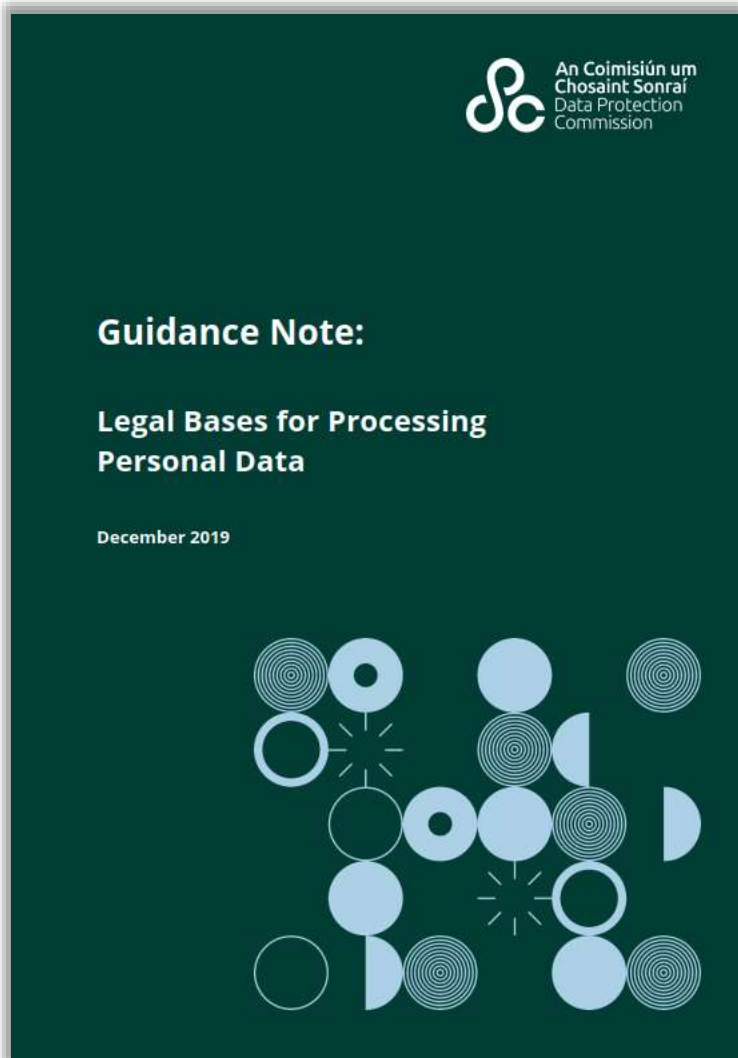
**5** Assess the **importance** of the objective and **whether the measure meets the objective**.

**6** Assess the **scope, the extent and the intensity of the interference**. - **SCOPE**: how many persons would be affected? - **EXTENT**: what type of data would be processed? for how long? - **INTENSITY**: would the measure allow precise conclusions to be drawn about private lives of individuals?

**7** Proceed to the **'fair balance' evaluation** of the measure.

**8** If the measure is **not proportionate**, identify and introduce **safeguards** (such as: reduce the scope or extent of personal data processing; introduce a sunset clause or an expiry term; provide for specific oversight/governance arrangements, etc.).

## Руководство DPC по определению правовой основы для обработки персональных данных



Ирландский надзорный орган Data Protection Commission в декабре 2019 года опубликовал руководство для контролеров по определению правильной правовой основы для той или иной обработки персональных данных и обязательств, которые соответствуют этой правовой основе.

	Right of Access	Right to Rectification	Right to Erasure	Right to Restriction	Right to Portability	Right to Object
Consent	✓	✓	✓	✓	✓	~ Can withdraw consent
Contract	✓	✓	✓	✓	✓	✗
Legal Obligation	✓	✓	✗	✓	✗	✗
Vital Interests	✓	✓	✓	✓	✗	✗
Public Task	✓	✓	✗	✓	✗	✓
Legitimate Interests	✓	✓	✓	✓	✗	✓

## Руководство CNIL по записи телефонных разговоров, подтверждающих заключение договора

**CNIL.**  
*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

### L'enregistrement des conversations téléphoniques afin d'établir la preuve de la formation d'un contrat

25 avril 2022

*De nombreux professionnels souhaitent conserver l'enregistrement d'un échange téléphonique avec un consommateur afin d'établir la preuve de la formation d'un contrat. Dans quelles conditions cet enregistrement peut-il être réalisé ? Quelles sont les garanties à apporter, notamment aux personnes concernées ?*



#### Quelles utilisations possibles ?

L'enregistrement de conversations téléphoniques à des fins de preuve de la formation du contrat est autorisé, sous réserve d'être nécessaires. Ainsi, un organisme souhaitant enregistrer des conversations téléphoniques à des fins probatoires doit, en tant que responsable de traitement, démontrer qu'il ne dispose pas d'autres moyens pour prouver qu'un contrat a été conclu avec la personne concernée.

Ainsi, il est nécessaire de distinguer les contrats qui peuvent être conclus à l'oral de ceux pour lesquels l'accord doit nécessairement se matérialiser par un acte écrit.

Французский орган по защите данных (CNIL) 25.04.2022 выпустил руководство по записи телефонных разговоров, подтверждающих заключение договора. В руководстве указано, что организации должны продемонстрировать отсутствие у них других способов доказывания факта заключения договора с субъектом данных, поэтому проводится различие между устными и письменными договорами. Кроме того, CNIL пояснил, что для телефонных записей должен соблюдаться принцип минимизации данных, а это означает, что записи не должны быть постоянными или систематическими. В дополнение к этому пункту CNIL подчеркнул, что следует записывать только разговоры, связанные с заключением договора, и поэтому должны быть предусмотрены механизмы, обеспечивающие запись только с того момента, когда ее цель явно связана с заключением договора.

## Руководство CNIL по повторному использованию данных процессором, доверенных ему контролером

**CNIL.**  
*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

### Sous-traitants : la réutilisation de données confiées par un responsable de traitement

12 janvier 2022

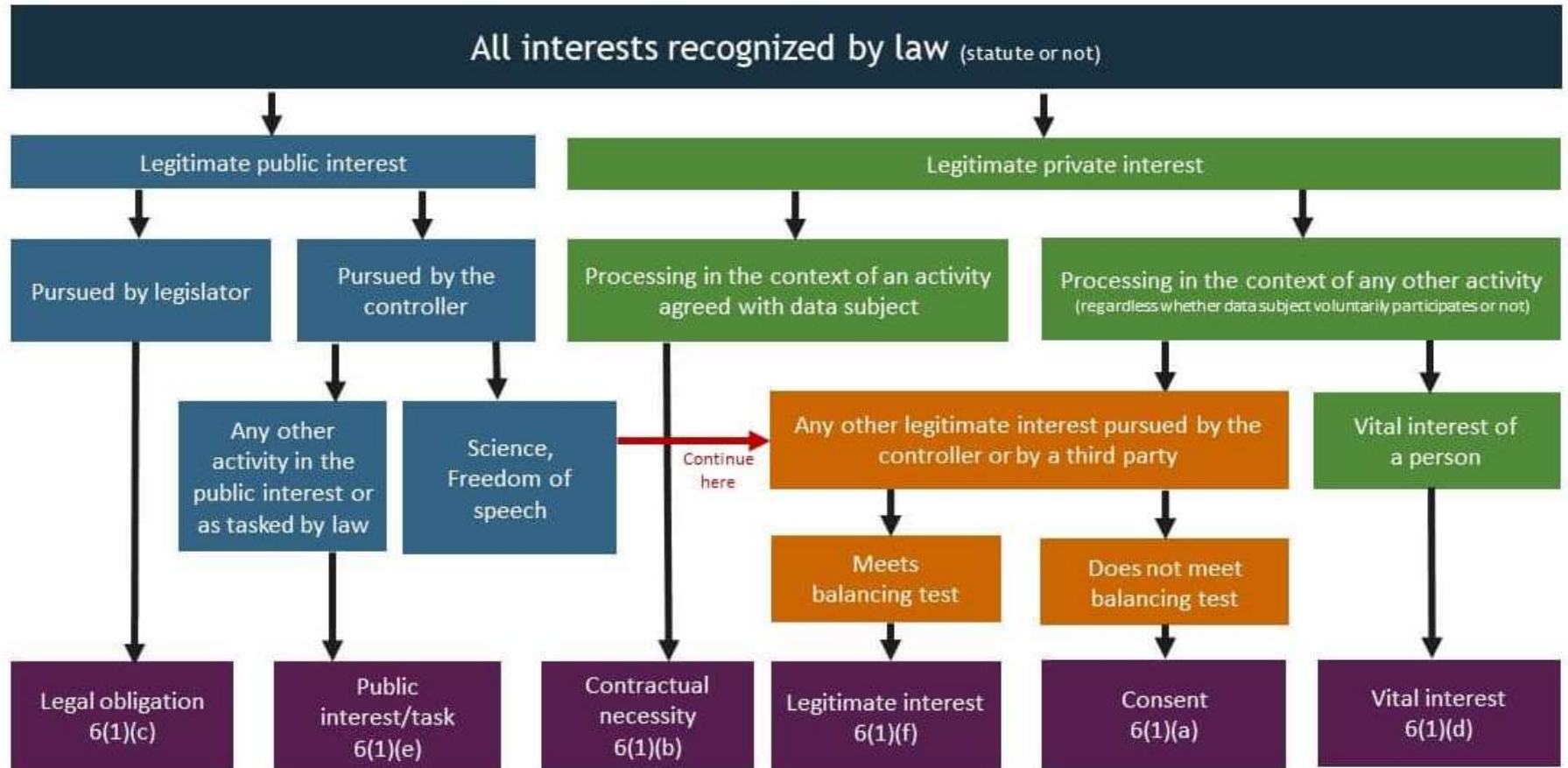
*Un sous-traitant ne peut réutiliser des données personnelles pour son propre compte que si cette réutilisation est compatible avec le traitement initial et que le responsable du traitement lui en a donné l'autorisation écrite.*



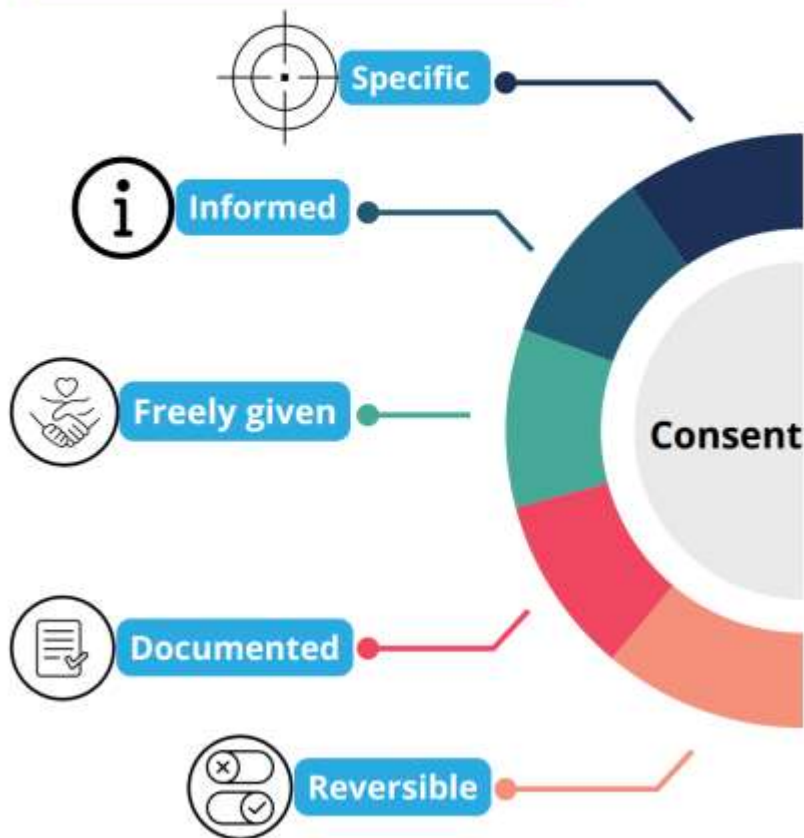
Selon la définition donnée par le règlement général sur la protection des données (RGPD), un **sous-traitant** traite des données personnelles pour le compte du responsable du traitement. Dans ce cadre, il ne fait que suivre les instructions du responsable de traitement et ne peut pas, en principe, utiliser les données pour son propre compte. Il arrive toutefois qu'un sous-traitant souhaite réutiliser les données avec souvent pour objectif l'amélioration de ses services ou de ses produits ou la conception de nouveaux services et produits. **Une telle réutilisation n'est possible qu'à plusieurs conditions.**

Французский надзорный орган по защите данных (CNIL) 12.01.2022 руководство по повторному использованию персональных данных процессором, доверенных ему контролером в рамках поручения. В соответствии с GDPR процессоры, обрабатывающие персональные данные от имени контролера, должны делать это только в соответствии с инструкциями контролера и в принципе не могут использовать данные в своих собственных целях. Однако CNIL отметил, что часто процессоры могут захотеть повторно использовать такие данные, например, с целью улучшения своих услуг или продуктов или разработки новых услуг и продуктов, и что это действительно возможно при определенных обстоятельствах.

## Choosing the right legal basis in the GDPR



## GUIDANCE: Consent



2024 issue

### Asking for consent

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions or other matters.
- We ask people to positively opt in.
- We do not use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand and appropriate for the person we are asking for consent from.
- We are clear why we want the data and what we are going to do with it.
- We give individual ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent and explain how they can do it.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for children under 13 years of age) in place.

### Recording consent

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

# Модели предоставления согласия на обработку персональных данных и сопутствующие им риски

Privacy риски

Модели предоставления согласия

Вероятность

Способ выражения согласия

Форма получения согласия

Метод сбора согласия

низкая

**Double Opt-in**, дважды активно выраженное согласие. Например, субъект заполняет веб-форму на рассылку и нажимает кнопку «Согласен на обработку ПД», а потом на указанный субъектом адрес приходит электронное письмо с просьбой подтвердить согласие путем нажатия на гиперссылку в письме.

**Single Opt-in**, единожды активно выраженное согласие. Например, субъект проставляет «галочку» в пустом чек-боксе «Согласен на обработку ПД».

**Silent Opt-in**, пассивно выраженное согласие. Например, «галочка» в чек-боксе «Согласен на обработку ПД» уже предустановлена, а субъект не убирает её из чек-бокса, или когда субъект наживает кнопку отправления данных, которая сопровождается соответствующим предупреждением (*Нажимая кнопку «Отправить» Вы даете свое согласие...*).

**Soft Opt-out**, необременительный способ выражения несогласия. Например, в условия обслуживания включено согласие субъекта на обработку ПД, а также включен отдельный чек-бокс «Не согласен на обработку ПД», в котором субъект может проставить галочку.

**Hard Opt-out**, обременительный способ выражения несогласия. Например, субъекту направляется уведомление об обновлении условий обслуживания, в которые теперь включено согласие на обработку ПД, и если субъект не направит в установленный срок отказ (в письменной форме или по телефону), то согласие считается предоставленным.

**Письменная** – используется бумажный носитель информации (например, договор), который собственноручно подписывается субъектом.

**Электронная** – субъект подтверждает свое согласие с помощью квалифицированной (КЭП), неквалифицированной (НЭП) или простой электронной подписи (ПЭП). С субъектом необходимо заключить предварительное письменное соглашение о легализации НЭП/ПЭП.

**Конклюдентная** – субъект своими действиями (поведением) показывает свое желание и готовность разрешить обработку персональных данных.

**Устная** - заявление (выражение) субъектом своего согласия как очно, так и с использованием средств голосовой связи. Риск снижается путем записи разговора и/или дополнительной верификации субъекта (например, получением ответного sms-сообщения).

**Отдельный документ или текст.**

**Составная часть иного документа** (анкеты, заявления, согласия).

**Составная часть договора с субъектом.**

высокая



## Sample LIA template



This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our [legitimate interests guidance](#).

### Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (eg, profiling requirements, or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

### Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

- Will this processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?
- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

### Part 3: Balancing test

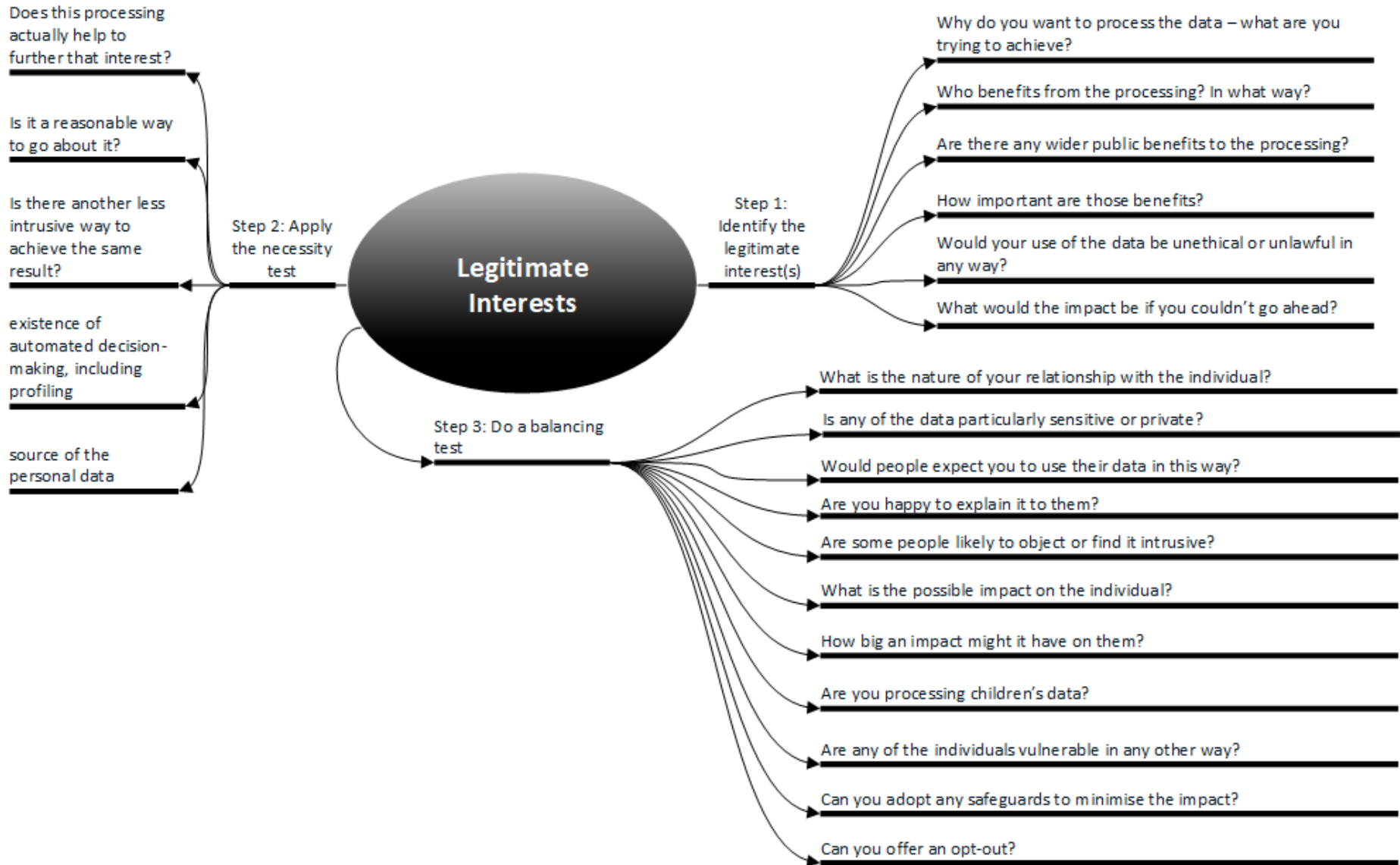
You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the [DPIA screening checklist](#). If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

## Checklists

- We have checked that legitimate interests is the most appropriate basis.
- We understand our responsibility to protect the individual's interests.
- We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
- We have identified the relevant legitimate interests.
- We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.
- We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.
- We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
- We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
- If we process children's data, we take extra care to make sure we protect their interests.
- We have considered safeguards to reduce the impact where possible.
- We have considered whether we can offer an opt out.
- If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
- We keep our LIA under review, and repeat it if circumstances change.
- We include information about our legitimate interests in our privacy information.

## 106 Схема проведения Legitimate Interests Assessment



## Руководство DPN по использованию Legitimate Interests и проведению LIA



### Understanding what Legitimate Interests are

Key definitions

The Lawful Basis for processing under the GDPR

Individuals' rights under the GDPR & the implications of using Legitimate Interests

### Identifying areas of processing where Legitimate Interests may apply

How Legitimate Interests might apply

Case studies & examples of where Legitimate Interests may apply

### The Legitimate Interests Assessment (LIA) - the 3 stage test

Identifying a Legitimate Interest

The 'necessity test'

The 'balancing test'

### Transparency and the consumer

How to communicate the use of Legitimate Interests effectively and transparently to individuals

### Appendices:

Appendix A – Legitimate Interest Process Flow for selecting Lawful Basis for processing

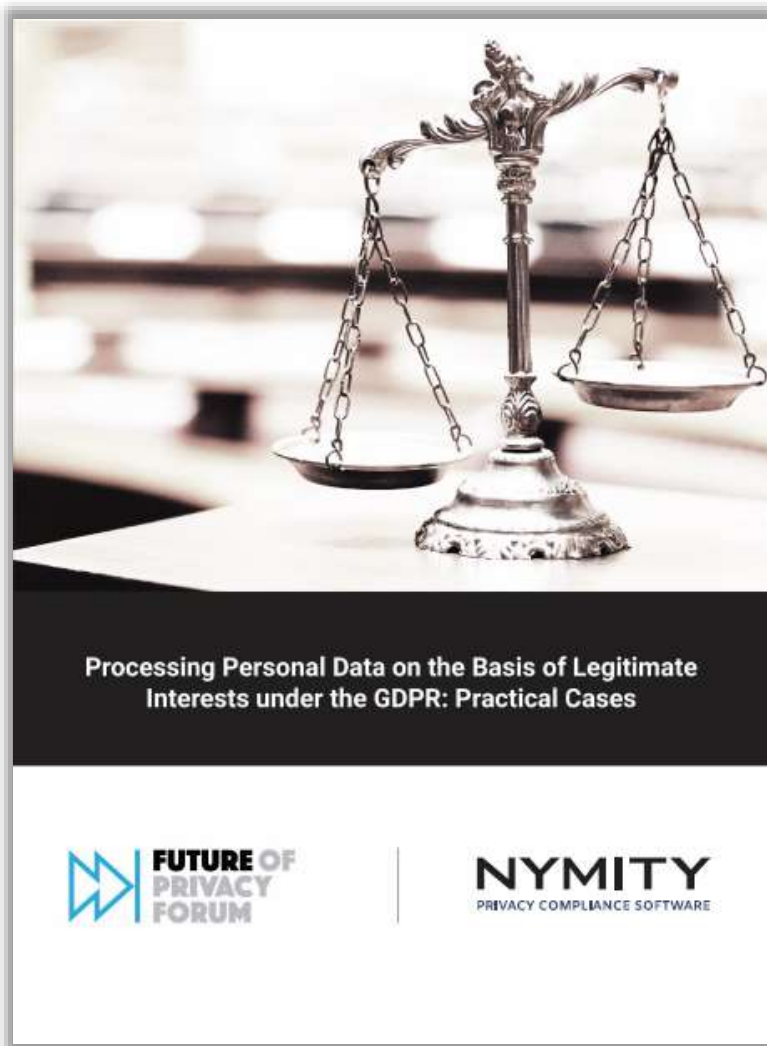
Appendix B – Legitimate Interests Assessment Template

Appendix C - Legitimate Interests Assessment Example

Appendix D – The GDPR articles and recitals relating to Legitimate Interests

Appendix E – Glossary of terms

## Обработка персональных данных на основании Legitimate Interests: правоприменительная и судебная практика



Future of Privacy Forum и NYMITY подготовили обзор европейской правоприменительной и судебной практики в сфере обработки данных на основании законного интереса (legitimate interests). Обзор затрагивает как решения национальных органов по защите данных (DPAs) и судов Европейского экономического пространства (EEA), а также наиболее значимые решения Суд Европейского Союза (Court of Justice of the European Union). Практика была разделена на две части: в первой описаны решения о законности использования legitimate interests в качестве правового основания для обработки персональных данных, а во второй – когда решение было обратным.

Обзор содержит полезные примеры «упражнения по балансировке» законных интересов, а также описание корректирующих мер, необходимые для изменения баланса и придания законности обработки данных.

## Investigating Deceptive Design in GDPR's Legitimate Interest

Lin Kyi  
Max Planck Institute for Security and  
Privacy  
Bochum, Germany  
lin.kyi@mpi-sp.org

Sushil Ammanaghatta  
Shivakumar  
Max Planck Institute for Security and  
Privacy  
Bochum, Germany  
sushil.shivakumar@mpi-sp.org

Franziska Roesner  
University of Washington  
Seattle, United States  
franz@cs.washington.edu

Cristiana Santos  
Utrecht University  
Utrecht, Netherlands  
c.teixeirasantos@uu.nl

Frederike Zufall  
Max Planck Institute for Research on  
Collective Goods  
Bonn, Germany  
zufall@coll.mpg.de

Asia J. Biega  
Max Planck Institute for Security and  
Privacy  
Bochum, Germany  
asia.biega@mpi-sp.org

### ABSTRACT

Legitimate interest is one of the six grounds for processing data under the European Union's General Data Protection Regulation (GDPR). The flexibility and ambiguity of the term "legitimate interests" can be problematic, coupled with the lack of enforcement from legal authorities and different interpretations from the various data protection authorities, legitimate interests can be taken advantage of as a loophole to collect more user data.

Drawing insights from multiple disciplines, we ran two studies to empirically investigate the deceptive design used when legitimate interests are applied in privacy notices, and how user perceptions line up with practice. We identified six deceptive designs, and found that the ways legitimate interest is applied in practice does not line up with user expectations.

### CCS CONCEPTS

• Security and privacy → Human and societal aspects of security and privacy; • Human-centered computing → User studies; • Applied computing → Law.

### KEYWORDS

Deceptive Design, Dark Patterns, GDPR, Consent, Privacy Notice, Legitimate Interest, Human-Computer Interaction

### ACM Reference Format:

Lin Kyi, Sushil Ammanaghatta Shivakumar, Franziska Roesner, Cristiana Santos, Frederike Zufall, and Asia J. Biega. 2023. Investigating Deceptive Design in GDPR's Legitimate Interest. In *Proceedings of ACM CHI Conference on Human Factors in Computing Systems* (CHI '23). ACM, New York, NY, USA, 13 pages. <https://doi.org/10.1145/3589000.3589000>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions.acm.org](https://permissions.acm.org).

CHI '23, April 23–28, 2023, Hamburg, Germany  
© 2023 Association for Computing Machinery  
ACM ISBN 978-1-609-59255-5/23/00...\$11.00  
<https://doi.org/10.1145/3589000.3589000>

### 1 INTRODUCTION

The European Union's General Data Protection Regulation (GDPR) outlines legal grounds for the processing of personal data to be lawful (Article 6), including the legal basis of consent and legitimate interest, amongst other grounds [14]. Legitimate interest is defined in Article 6(1)(f) of the GDPR as the processing that is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party" [14, 19]. Pursuant to this paper, data controller refers to a website or company that is processing personal data, such as service providers, advertisers, and consent management platforms (CMPs) [69].

While the practical implementations of the legal basis of consent have already been studied in a variety of contexts [40, 51, 60, 69], the usage of legitimate interests as a legal basis for data processing by websites remains relatively unexplored. Yet, as highlighted by legal scholars, one of all legal grounds under the GDPR, legitimate interest is the most ambiguous one because it allows for broad interpretations of different processing purposes [28, 44]. In fact, the legal uncertainty of which data processing purposes should fall under the legal basis of legitimate interest is currently the subject of great attention at the EU level by the European Commission [25], Data Protection Authorities (DPAs) [18, 19], the EU Court of Justice (ECJ) [17], as well as other national courts. Moreover, the lack of legal enforcement from regulators and courts may allow for this legal basis to be exploited by data controllers as a loophole for dubious data practices [28, 44]. Hence, there is a need for further investigation into the use and applicability of legitimate interests in practice.

Even though legitimate interests allow data controllers to process data without explicit permission from the user, they have the right to object to legitimate interests (Art. 21(1) GDPR). As a result, legitimate interests appear in website privacy notices more and more commonly (see Figure 1 for an example notice design). The potential for legitimate interest to be exploited to collect more user data raises the question of whether its practical implementations use any deceptive design. In the context of consent, it has been shown

"The notices we focus on this paper are also often called 'variant notices', 'cookie banners', or 'cookie pop-ups'. We use the term 'privacy notices' just to be consistent with 'privacy policies' here, since we refer to notices that do not just ask for consent but also inform users of data processing based on legitimate interests."

Законный интерес является одним из шести оснований для обработки данных в соответствии с Общим регламентом о защите данных Европейского союза (GDPR). Гибкость и неоднозначность термина "законный интерес" может быть проблематичной; в сочетании с отсутствием правоприменения со стороны юридических органов и различными интерпретациями со стороны различных органов по защите данных, законные интересы могут быть использованы в качестве лазейки для сбора большего количества пользовательских данных.

Используя знания из различных дисциплин, авторы провели два исследования, чтобы эмпирически изучить обманные конструкции, используемые при применении законных интересов в уведомлениях о конфиденциальности, и то, как восприятие пользователей согласуется с практикой. Выявлено шесть недобросовестных конструкций и обнаружено, что способы применения законных интересов на практике не совпадают с ожиданиями пользователей.

## Обзор от CIPL по примерам использования Legitimate Interests в качестве правового основания обработки



27 April 2017

### CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data

#### Discussion Draft

In preparation for CIPL GDPR Project Madrid Workshop III, CIPL has asked the GDPR project members for examples where a) legitimate interest is the appropriate ground for processing personal data, and b) in some cases the only legal ground for processing.

The purpose of the exercise was to establish current practices and instances of organisations using legitimate interest processing under the current law and to inform all the stakeholders involved in the GDPR implementation of the broad application of this ground of processing today.

Part I of this document is a summary of the examples we received, organised in broad categories of processing purposes. Part II are specific case studies from different industry sectors that provide an in-depth discussion of the rationale for legitimate interest processing, and the balancing of interests and risk mitigation undertaken by the controller to ensure accountability and to meet the reasonable expectations of the individual.

The examples we received demonstrate the following:

- a) organisations in all sectors currently use legitimate interest processing for a very large variety of processing personal data and this trend is likely to continue under the GDPR.
- b) in many cases, legitimate interest processing is the most appropriate ground for processing, as it entails organisational accountability and enables responsible uses of personal data, while effectively protecting data privacy rights of individuals.
- c) in some cases, organisations use legitimate interest as the only applicable ground for processing, as none of the other grounds can be relied on in a particular case.
- d) organisations using legitimate interest always consider the interest in case (of controller or a third party / parties); they balance the interest with the rights of individuals; and they also apply safeguards and compliance steps to ensure that individuals rights are not prejudiced in any given case.
- e) the current use cases of legitimate interest tend to form a pattern, with most common examples being prevalent in many organisations and all the cases broadly falling in several wide categories outlined below. The most prevalent category of legitimate interest cases across all industries is i) fraud detection and prevention and ii) information and system security.

Centre for Information Policy Leadership предлагает обзор практики и примеров опоры на законный интерес при обработке персональных данных в следующих областях:

1. Fraud detection and prevention (crime prevention);
2. Compliance with foreign law, law enforcement, court and regulatory bodies' requirements;
3. Industry watch-lists and industry self-regulatory schemes;
4. Information, system, network and cyber security;
5. Employment data processing;
6. General Corporate Operations and Due Diligence;
7. Product development and enhancement;
8. Communications, marketing and intelligence.

## Отчет от AEPD об использовании Legitimate Interests для обработки данных в кредитных организациях



Gabinete Jurídico

N/REF: 028891/2019

La consulta se centra en la licitud de un tratamiento de datos en un sistema de información crediticia que contendrá tanto información relativa al cumplimiento de obligaciones dinerarias (información positiva) como información relativa al incumplimiento de dichas obligaciones (información negativa), al amparo de la base jurídica contemplada en el artículo 6.1.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos, RGPD).

Esta cuestión ha sido objeto de estudio por este Gabinete Jurídico, desde la perspectiva más amplia que permitía el análisis del Código de conducta del sector infomediario de protección de datos de carácter personal presentado por la Asociación Multisectorial de la Información (ASEDIE), y que se ha informado desfavorablemente en nuestro reciente informe 89/2020, de 16 de marzo de 2021, siendo sus argumentos relativos al tratamiento de datos personales por los denominados "ficheros positivos" sobre la base jurídica del artículo 6.1.f) del RGPD, plenamente trasladables a la presente consulta, por lo que se procede a su transcripción:

### **I.- MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN CREDITICIA CON DATOS RELATIVOS AL CUMPLIMIENTO DE OBLIGACIONES DINERARIAS, FINANCIERAS O DE CRÉDITO (FICHEROS DE SOLVENCIA POSITIVOS).**

El informe emitido por la Subdirección General RGPD considera que su contenido no se adecúa a lo dispuesto en el RGPD o en la LOPDGDD, enumerando una serie de razones que se sintetizan en las siguientes: se aprecia una confusión entre el interés del responsable y la finalidad del tratamiento, ya que el interés invocado no parece ser sino el de obtener un beneficio económico en tanto que la necesidad de que terceras entidades conozcan los datos de cumplimientos económicos constituiría la finalidad del tratamiento; los datos se recabaron con otra finalidad, debiendo concluirse que el juicio o test de compatibilidad sería contrario al principio de finalidad; el artículo 5 del RGPD requiere que los datos sean tratados de manera lícita, leal y transparente en relación con el interesado y el interés legítimo exige que el tratamiento sea necesario; de los datos tratados se puede llegar a obtener un perfil de los interesados que muestre su vida e intimidad personal y familiar;

Испанский орган по защите данных (AEPD) опубликовал 19.04.2021 отчет, в котором анализируется возможность обработки данных, касающихся выполнения клиентами кредитных организаций своих денежных обязательств (т.е. положительная информация) и несоблюдения этих обязательств (т.е. отрицательная информация), на основании законных интересов кредитных организаций в соответствии со ст.6(1)(f) GDPR.

В этой связи в отчете подчеркивается, что обработка положительной информации о клиентах не может быть основана на законных интересах кредитных организаций, поскольку указанная статья GDPR и применимое законодательство Испании явно регулируют только обработку негативной информации о клиентах.

## Европейская комиссия критикует интерпретацию законного интереса голландским DPA



Европейская комиссия (ЕК) в инициативном порядке обратилась к голландскому Управлению по защите данных (DPA) с критикой его трактовки законного интереса в соответствии с GDPR.

Критика прозвучала в ответ на правоприменительные действия и руководство, выпущенное голландским DPA, в котором говорится, что обработка данных в чисто коммерческих интересах никогда не может быть основана на законных интересах компании. ЕК считает, что такое толкование является слишком строгим и противоречит GDPR, прецедентному праву Суда ЕС и руководству Рабочей группы по статье 29 (WP29) и Европейского совета по защите данных (EDPB). Фактически, ЕК считает, что данная интерпретация препятствует предпринимательской деятельности, поскольку она существенно ограничивает возможности предприятий по обработке персональных данных в коммерческих интересах.

ЕК предложила голландскому DPA изменить свою точку зрения, но пока голландский DPA заявил, что остается на своей позиции.



## Итальянский Garante и испанский AEPD начали расследование против TikTok из-за рекламы на основе законного интереса



**GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

**Provvedimento del 7 luglio 2022**

[VEDI ANCHE COMUNICATO STAMPA DELL'11 LUGLIO 2022](#)

[doc. web n. 9788429]

Provvedimento del 7 luglio 2022

Registro dei provvedimenti  
n. 248 del 7 luglio 2022

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stazione, presidente, la prof.ssa Ginevra Carrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il dott. Fabio Mattei, segretario generale;

VISTA la direttiva 2002/58/CE del 12 luglio 2002, del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (di seguito "Direttiva ePrivacy");

VISTA la direttiva 2009/136/CE del 25 novembre 2009, del Parlamento europeo e del Consiglio, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), come modificato dal d.lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al citato Regolamento (di seguito "Codice");

VISTO il Parere del Gruppo di lavoro Articolo 29 n. 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'art. 7 della Direttiva 95/46/CE);

VISTO il Parere del Comitato europeo per la protezione dei dati personali n. 05/2019 sulle interrelazioni tra la direttiva e-Privacy ed il Regolamento, con particolare riguardo alle competenze, ai compiti ed ai poteri delle Autorità di protezione dati;

VISTE le linee guida del Gruppo di lavoro Articolo 29 del 6 febbraio 2018, sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento

В июне 2022г. TikTok объявил о предстоящих изменениях в политике конфиденциальности и о своем намерении начать с 13.07.2022 профилирование и показ персонализированной своим пользователям старше 18 лет. Согласно позиции TikTok, такая обработка персональных данных будет основана на законных интересах TikTok, его рекламных партнеров и пользователей, в соответствии со статьей 6(1)(f) GDPR, а не на согласии субъектов данных.

Итальянский орган по защите данных ("Garante") 07.07.2022 вынес срочное предупреждение в отношении TikTok Italy S.r.l. и TikTok Technology Limited. и TikTok Technology Limited за предполагаемые нарушения ст.5(3) ePrivacy Directive и ст.6(1)(f) GDPR.

Испанский орган по защите данных ("AEPD") 12.07.2022 инициировал аналогичное расследование в отношении TikTok Technology Limited.

## Рекомендации IAB Europe по осуществлению LIA в контексте цифровой рекламной деятельности



### Appendix A: Common risks in the digital advertising industry

This is a non-exhaustive list of common risks from processing activities in the digital advertising industry, with some particular considerations relative to each. It is provided as a useful reference. You should take care to think about risks to data subjects' rights and freedoms present in your circumstances that may not be represented here.

For your own LIA you will need to analyse the impact and likelihood of the specific risks you identify. Some types of risk will have a more harmful impact on data subjects, if they are realised, than others, and you should take that into account in your analysis. Data protection authorities will take this factor into account themselves when determining the appropriate level of regulatory action in the event of an infringement/breach.

Risk	Considerations
<i>Expectations and rights of the data subject</i>	
Data subject would not expect the processing	Is the processing something data subjects expect or would they be surprised? Do you have an existing relationship with the data subject that may affect this? Particular things that could cause surprise include, for example, processing across seemingly unrelated contexts, matching data from different sources, cross-device, household, and social graphing. Providing sufficient information and transparency into the processing can help ensure data subjects are not surprised.
Embarrassment	Could a data subject feel embarrassed if, for example, they receive an ad based on web browsing on a sensitive topic? What if someone else sees the ad, or the ad is delivered across a device graph?
Unwanted disclosure	Could data about the data subject be disclosed to other parties in ways that the data subject would be surprised by and wouldn't want? For example, could browsing history be matched to a retailer's CRM data?
Discomfort – a feeling of privacy invasion	Users may be made uncomfortable by certain processing, when they become aware of it. For example, many users feel discomfort when they are retargeted. The level of intrusion into a user's privacy should be considered in assessing the impact of the risk.

<https://iab europe.eu/blog/gdpr-guidance-legitimate-interests-assessments-lia-for-digital-advertising/>

<https://iab europe.eu/wp-content/uploads/2021/03/IAB-Europe-GDPR-Guidance-Legitimate-Interests-Assessments-LIA-for-Digital-Advertising-March-2021.pdf>



**Методические рекомендации RPPA по вопросам обработки персональных данных, необходимой для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных**

*Редакция 1.0 от 29.10.2020г.*

## Введение

В соответствии с ч. 1 ст. 5 и ч. 1 ст. 6 Федерального закона "О персональных данных" от 27 июля 2006 г. № 152-ФЗ (далее "Закон"), одним из основополагающих принципов обработки персональных данных является допустимость обработки персональных данных исключительно на законной и справедливой основе и исключительно при наличии одного из предусмотренных Законом правовых оснований.

Так, обработка персональных данных может осуществляться, например:

- (а) с согласия субъекта персональных данных на обработку его персональных данных, которое должно являться конкретным, информированным и сознательным и может быть дано только в позволяющей подтвердить факт его получения форме;
- (б) для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- (в) если обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; и т.п.

П. 7 ч. 1 ст. 6 Закона, среди прочих правовых оснований, допускает обработку персональных данных в случаях, когда она необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.



## Приложение 2

### Примеры из практики Европейского Союза / государств Европейской Экономической Зоны

**Примеры случаев, когда ссылки на законный или общественный интерес были признаны обоснованными**

1. Оценка кредитоспособности клиентов<sup>10</sup>
2. Передача данных внутри группы компаний для предотвращения мошенничества и для внутренних административных целей<sup>11</sup>
3. Обеспечение сетевой и информационной безопасности, например предотвращение несанкционированного доступа к коммуникационным сетям, вредоносного кода, атак типа «отказ в обслуживании» и повреждения компьютерных и электронных систем связи<sup>12</sup>
4. Получение данных о лице, причинившем ущерб собственности, с целью предъявления иска этому лицу о возмещении ущерба<sup>13</sup>
5. Проведение проверок биографии и репутации перед началом делового сотрудничества<sup>14</sup>
6. Ведение домашнего видеонаблюдения с целью защиты имущества, здоровья и жизни жителей дома<sup>15</sup>
7. Обработка сведений о привлечении к уголовной ответственности в рамках сервиса проверки биографических данных сотрудников, предоставляемого специализированным поставщиком для работодателей<sup>16</sup>
8. Мониторинг доступа сотрудников к информационным системам банка для защиты информации ограниченного доступа и обеспечения безопасной и бесперебойной работы ИТ-систем<sup>17</sup>
9. Раскрытие медицинских данных больницей по запросу адвоката в судебных целях<sup>18</sup>
10. Раскрытие работодателем персональных данных должника коллектору в отношении долга<sup>19</sup>
11. Взыскание задолженности клиента перед банком и передача данных клиента субподрядчику (коллектору) банка<sup>20</sup>

<sup>10</sup> AEPD, Gabinete Jurídico, Informe 0195/2017.

<sup>11</sup> AEPD, Gabinete Jurídico, Informe 0195/2017.

<sup>12</sup> AEPD, Gabinete Jurídico, Informe 0195/2017.

<sup>13</sup> CJEU, Case C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtošanas policijas pārvalde v. Rīgas pašvaldības SIA "Rīgas satiks", 4 May 2017.

<sup>14</sup> Case C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, judgment from 9 March 2017.

<sup>15</sup> CJEU Case C-212/13 Fransson Rymäs v. Urad pro ochranu osobních údajů, 11 December 2014.

<sup>16</sup> Dutch DPA ([https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/omzetexpressie\\_nadecco.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/omzetexpressie_nadecco.pdf))

<sup>17</sup> DPA Monaco (<https://www.ccn.mc/images/documents/18a578936b7809a531f6d112c5c57467-Delub-2017-068-Andbank-habitatronics.pdf>)

<sup>18</sup> DPA Greece (<http://www.dpa.gr/APDPX/Portlets/htdocs/documentDisplay.jsp?docId=1108.123.017.01.201206.75>)

<sup>19</sup> DPA, Bulgaria ([https://www.cdpd.bg/index.php?menuitem\\_view&id=1480](https://www.cdpd.bg/index.php?menuitem_view&id=1480))

<sup>20</sup> Commission for Data Protection, Bulgaria - Decision No. ZH-07/2014 - Decision on Complaint Regarding Debt Collection

([https://www.cdpd.bg/index.php?menuitem\\_view&id=1346](https://www.cdpd.bg/index.php?menuitem_view&id=1346))

# Data Protection (Privacy) by Design and by Default



Термин «приватность» — калька с английского *privacy*, которое, в свою очередь, появилось в конце XIX века как отражение желания уединиться и защитить личное пространство в ответ на развитие технологий, в частности фотографии. Под приватностью в самом общем смысле понимают неприкосновенность частной и личной жизни. Выделяют несколько видов приватности: телесную, пространственную, информационную и коммуникационную, и все они актуальны в цифровом мире.



**Необходимость обеспечения приватности потребовала мультидисциплинарного подхода к защите персональных данных при их обработке в информационных системах. Воплощением этого подхода стала концепция PbDD: Privacy by Design (проектируемая приватность) и Privacy by Default (приватность по умолчанию).**

## 118 Data Protection (Privacy) by Design and by Default

### Проектируемая защита персональных данных (privacy by design)

- Принцип призван решить проблему «недальновидности» контролеров, которые должны заблаговременно продумывать механизмы защиты персональных данных на этапе планирования процедур их обработки в бизнес-активностях и ИТ-системах. Принцип должен быть внедрен в процессы жизненного цикла разработки системы (SDLC), управления изменениями, а так же в процессы проектного управления.
- Следуя этому принципу, контролеры перед запуском новых (модификацией уже существующих) бизнес-активностей/ИТ-систем должны проанализировать возможные риски для субъектов персональных данных с точки зрения возможности реализации их прав на доступ к своим данным, актуализации обрабатываемых данных, прекращения обработки данных и т.д.
- Дополнительно оценивается возможный вред субъектам персональных данных (privacy impact assessment), который может быть им нанесен в случае нарушения конфиденциальности персональных данных и безопасности их обработки.

### Защита персональных данных по умолчанию (privacy by default)

- Суть принципа: минимизация активностей по обработке персональных данных – чем меньше объем обрабатываемых данных, меньше способов и сроков их обработки, меньше круг вовлечённых в обработку третьих лиц, тем безопасней для субъектов данных и самого контролера.
- Минимизация обработки персональных данных позволяет вывести часть бизнес-процессов из-под регулирования законодательства о персональных данных и тем самым сэкономить силы и средства для контролеров.
- Принцип Privacy by default требует от контролеров соблюдать принцип подотчетности (accountability principle), то есть знать в каких процессах и ИТ-системах обрабатываются данные, в каком объеме, с какой целью и как долго.

119 7 основополагающих принципов PbDD от Энн Кавукян



1. **Стратегии, ориентированные на данные**, имеют скорее технический характер и фокусируются на обработке персональных данных с учетом требований приватности: **минимизация, сокрытие, разделение, объединение**.
2. **Стратегии, ориентированные на процессы**, имеют организационный характер и ориентированы на определение процессов, обеспечивающих ответственное управление персональными данными: **информирование, контроль, принуждение, демонстрация**.

Стратегии проектируемой приватности проявляются в том числе как элементы пользовательского интерфейса, названные паттернами приватности (Privacy Patterns) и являющиеся способом превращения Privacy by Design в практические советы для разработки программного обеспечения.



Согласно философии Privacy by Design лучший способ снизить риски, связанные с приватностью, — это не создавать их. Чем меньше данных оператор данных собирает и обрабатывает, тем меньше риск нарушения прав и свобод субъектов данных, а также нанесения ущерба самому оператору.



## 121 Стратегии проектируемой приватности (2)

1. Стратегии, ориентированные на данные, т.е. они носят более технический характер и фокусируется на обработке персональных данных с учетом требований приватности:
  - I. **минимизация (minimise)** – ограничение сбора ПД, а также дальнейший отбор и исключение избыточных ПД из наборов данных с последующим удалением/уничтожением этих ПД;
  - II. **сокрытие (hide)** – смешивание, запутывание, маскирование или ограничение доступа к ПД для предотвращения их неправомерного раскрытия;
  - III. **отделение (separate)** – обособленное (изолированное) хранение наборов персональных данных с целью затруднить их неправомерное сопоставление и объединение;
  - IV. **объединение (aggregate/abstract)** – агрегирование или группировка ПД для максимального снижения степени их детализации, которая все еще будет позволять извлекать пользу из обработки ПД.
2. Стратегии, ориентированные на процессы, т.е. они носят более организационный характер и ориентированы на определение процессов, обеспечивающих ответственное управление персональными данными:
  - I. **информирование (inform)** – своевременное информирование, объяснение и уведомление субъектов ПД в отношении фактов обработки и защиты ПД;
  - II. **контроль (control)** – субъекты ПД должны иметь должную меру контроля над обработкой ПД путем предоставления и отзыва информированного согласия, а также путем реализации иных принадлежащих им прав интуитивно понятным и своевременным образом;
  - III. **принуждение (enforce)** – соблюдение оператором своих юридических и договорных обязательств в отношении обеспечения добросовестности и безопасности обработки ПД путем реализации надлежащих правовых, организационных и технических мер;
  - IV. **демонстрация (demonstrate)** – способность оператора продемонстрировать соблюдение своих юридических и договорных обязательств в отношении обеспечения добросовестности и безопасности обработки ПД с помощью аудита, журналирования и отчетности.

## 122 Реализация стратегий проектируемой приватности

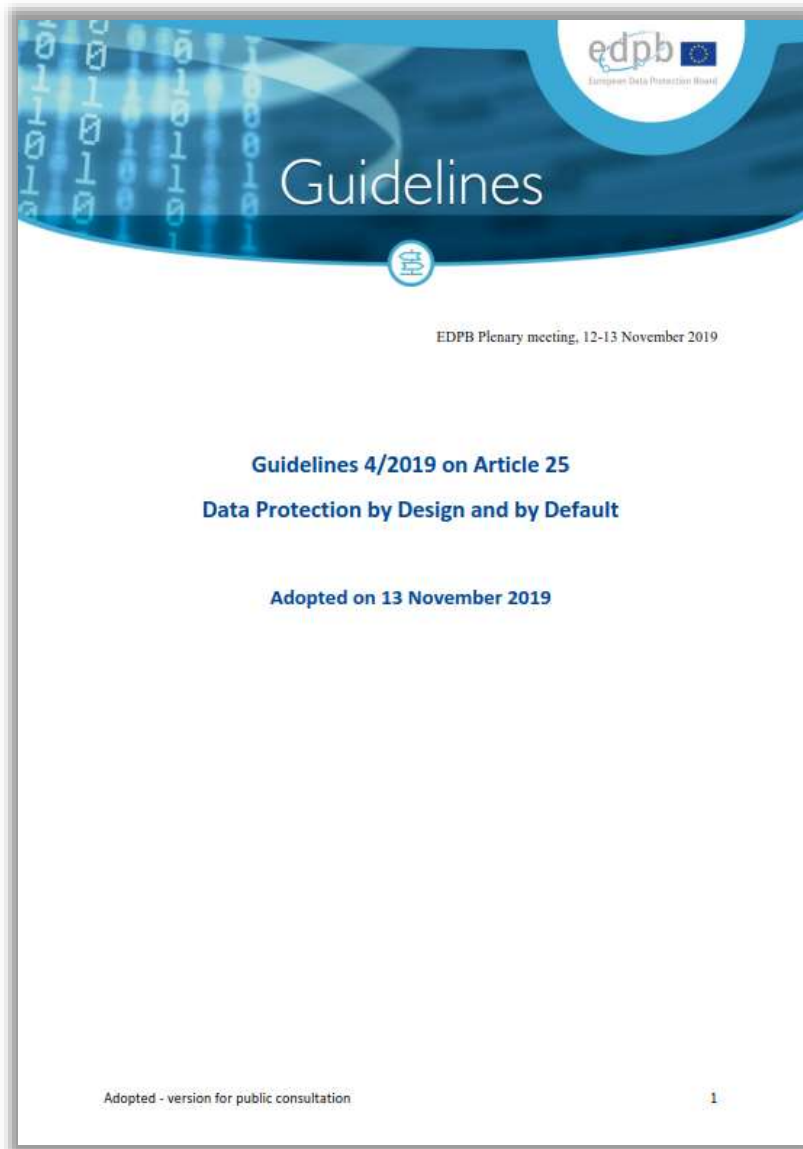




Суть принципа – минимизация процессов обработки данных. Чем меньше объем данных, чем меньше способов используется при их обработке, чем короче сроки и меньше круг вовлеченных лиц, тем безопасней обработка для субъектов данных и самого оператора. Минимизация позволяет вывести часть бизнес-процессов из-под действия законодательства о персональных данных и тем самым сэкономить силы и средства операторов.

- 1. Оптимизация** направлена на анализ обработки данных с точки зрения приватности, что означает принятие мер в целях минимизации объема собираемых данных, способов и длительности их обработки, а также степени их доступности.
- 2. Конфигурирование** (возможность настройки параметров обработки данных с помощью функций, доступных пользователю в приложениях, устройствах или системах) передает разумную часть этих параметров под контроль пользователя.
- 3. Ограничение** гарантирует, что обработка данных осуществляется с максимальным соблюдением приватности, поэтому настройки параметров должны быть установлены по умолчанию на значения, минимизирующие обработку персональных данных.

## 124 Руководство EDPB по Data Protection by Design and by Default

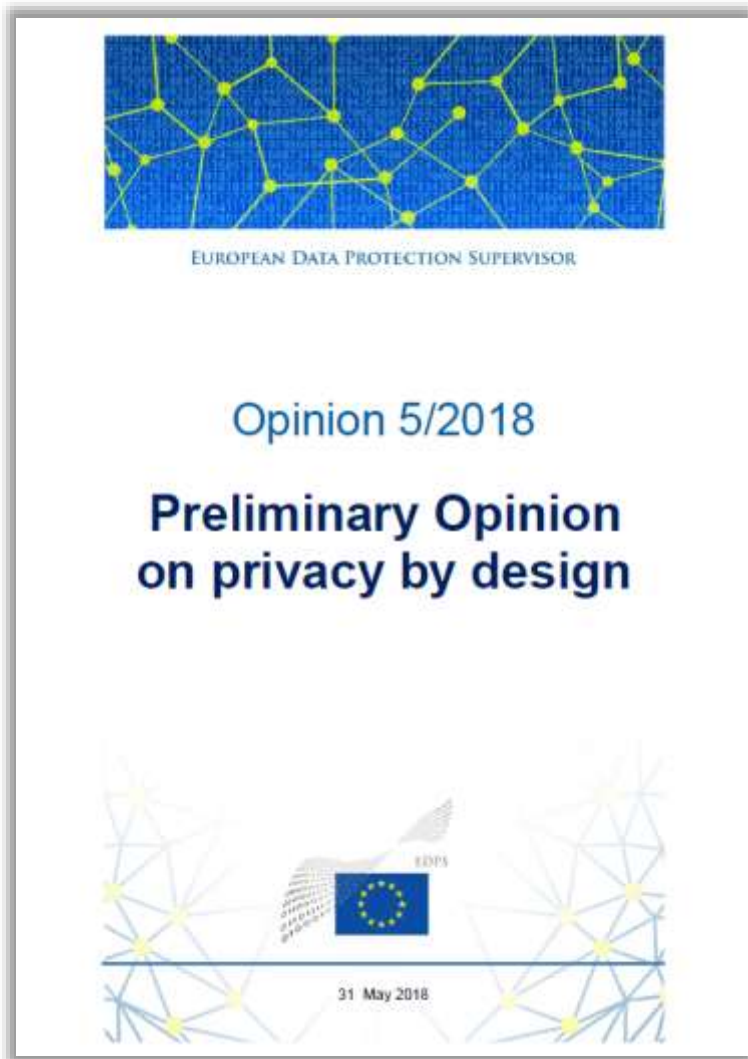


Европейский совет по защите данных (European Data Protection Board) опубликовал руководство 4/2019 по применимости ст.25 GDPR в контексте применения концептов Data Protection by Design and by Default.

Что необходимо принимать во внимание в DPIA:

- state of the art;
- cost of implementation;
- nature, scope, context and purpose of processing;
- risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

## Мнение EDPS от 2018 года о способах реализации принципов Privacy by Design



Опубликованный European Data Protection Supervisor документ направлен на то, чтобы способствовать надлежащей реализации обязательства по защите данных путем реализации принципов Data protection by design and by default, закрепленных в ст.25 GDPR. В документе приведен ряд практических рекомендаций, адресованных органам власти и организациям ЕС.

## Исследование от 2014 года по приватности и Data Protection by Design от ENISA



### *Privacy and Data Protection by Design – from policy to engineering*

December 2014



European Union Agency for Network and Information Security

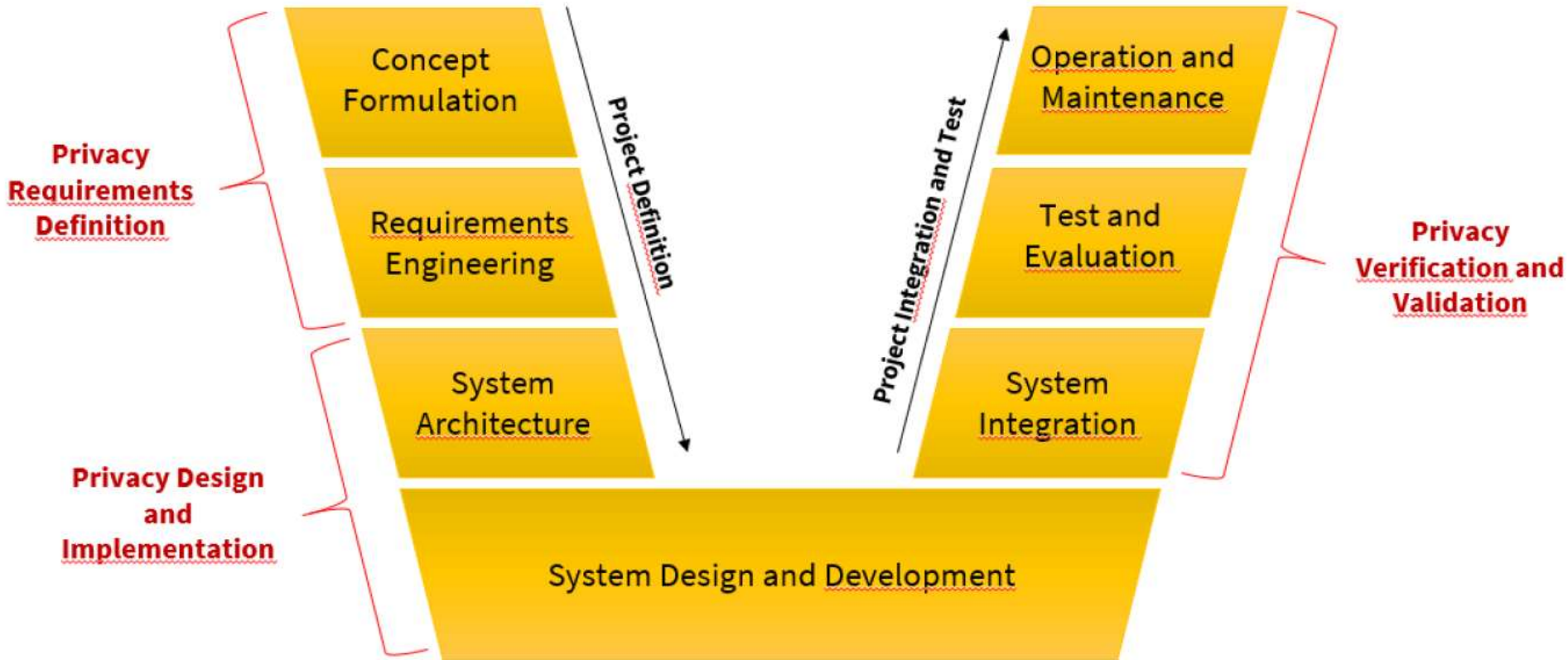
[www.enisa.europa.eu](http://www.enisa.europa.eu)

В этом исследовании представлен обзор способов и мер, которые могут быть использованы для преодоления разрыва между существующей правовой базой в сфере защиты персональных данных и имеющимися технологиями обработки информации. В документе описывается метод сопоставления юридических требований с проектными стратегиями, которые позволяют разработчику системы выбирать подходящие методы для реализации определенных требований конфиденциальности. Кроме того, в отчете отражены ограничения (как объективные, так и вызванные текущим уровнем техники) описываемого метода. Также приводятся рекомендации по преодолению и смягчению этих ограничений.



Агентство Европейского союза по кибербезопасности (ENISA) 26.01.2024 опубликовало отчет, в котором освещаются принципы проектирования защиты персональных данных в европейских пространствах данных. Пространства данных были описаны в Европейской стратегии данных на 2020 год, которая описывает "единое европейское пространство данных" как "настоящий единый рынок данных - открытый для данных со всего мира".

Инженерия защиты данных - это не просто инструмент обеспечения соответствия, но и возможность, среди прочего, усилить принципы защиты данных, обеспечить права субъектов данных, минимизировать риски неправомерного использования информации при обмене данными и снизить риск утечки данных. В докладе подробно описываются меры, включая использование технологий, повышающих конфиденциальность (PET), таких как анонимизация и псевдонимизация, но отмечается, что сотрудничество между держателями данных и посредниками данных имеет важное значение для реализации безопасного и законного обмена данными.

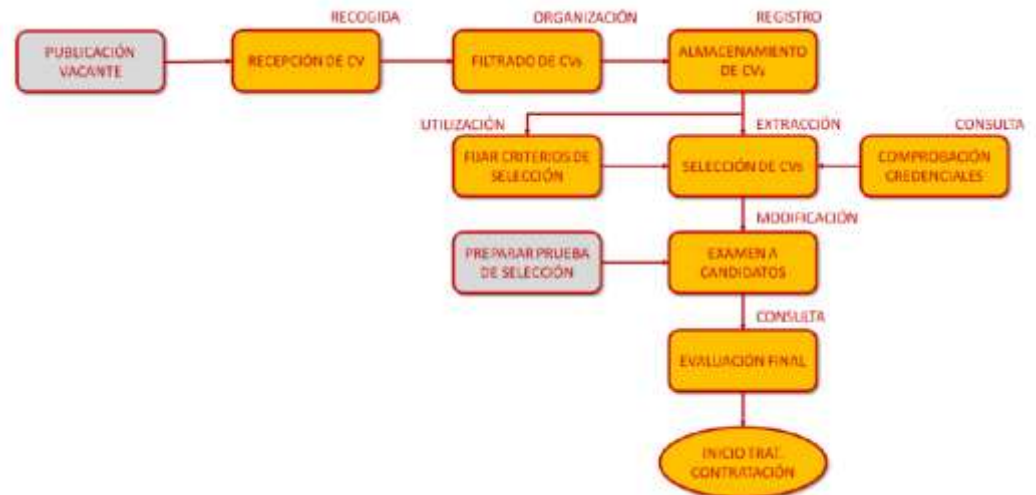




## 129 Практическое Руководство AEPD по Privacy by Default



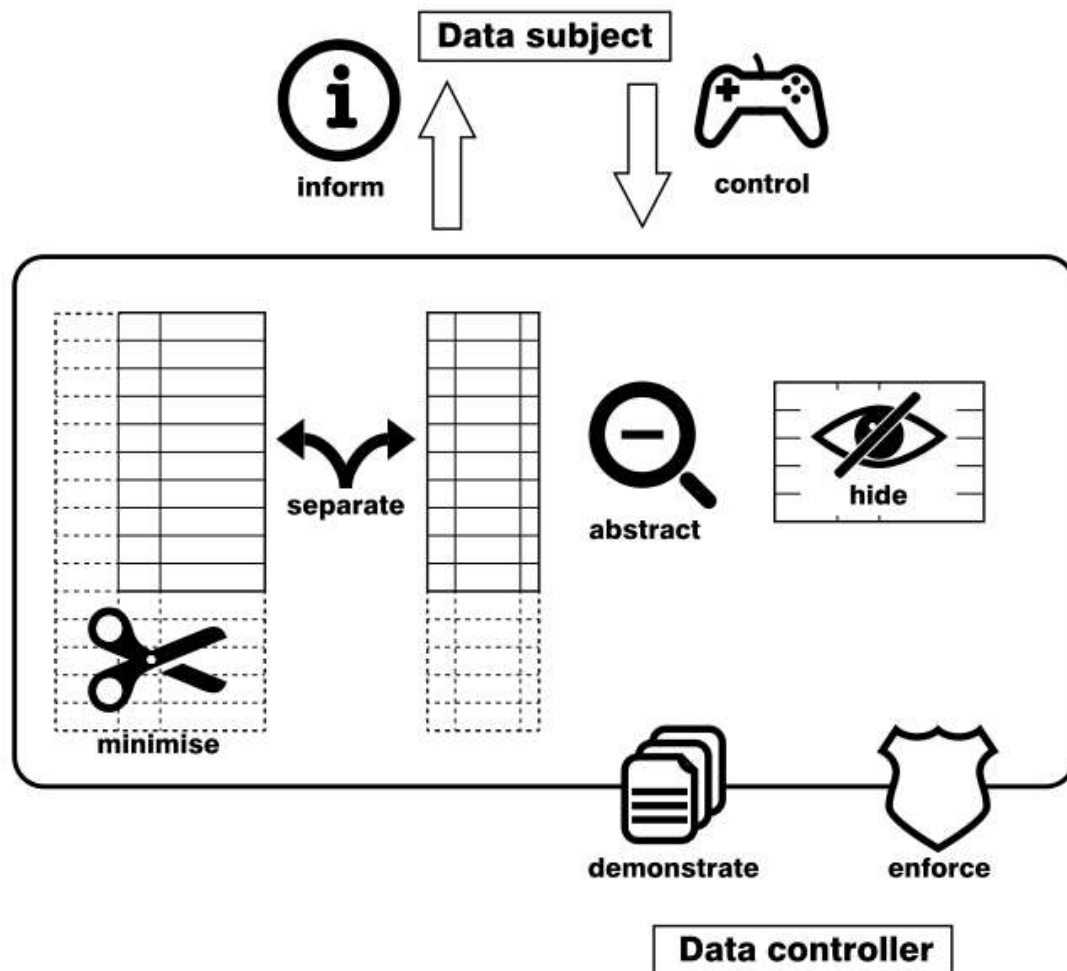
Испанский орган по защите данных (AEPD) выпустил 8 октября 2020 года руководство по практическому применению концепта Privacy by Default. В руководстве рассматриваются практические аспекты Privacy by Default, включая рекомендации по объему собираемых данных, сроку хранения и доступу к сохраняемым данным. Данный документ был подготовлен с учетом разъяснения Европейского совета по защите данных 4/2019 по ст.25 GDPR «Проектируемая защита данных и защита данных по умолчанию».



<https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf>

[https://rppa.ru/files/aepd\\_protection\\_by\\_default.pdf](https://rppa.ru/files/aepd_protection_by_default.pdf) - перевод на английский

## Практическое Руководство норвежского Datatilsynet по Data Protection by Design and by Default при разработке ПО

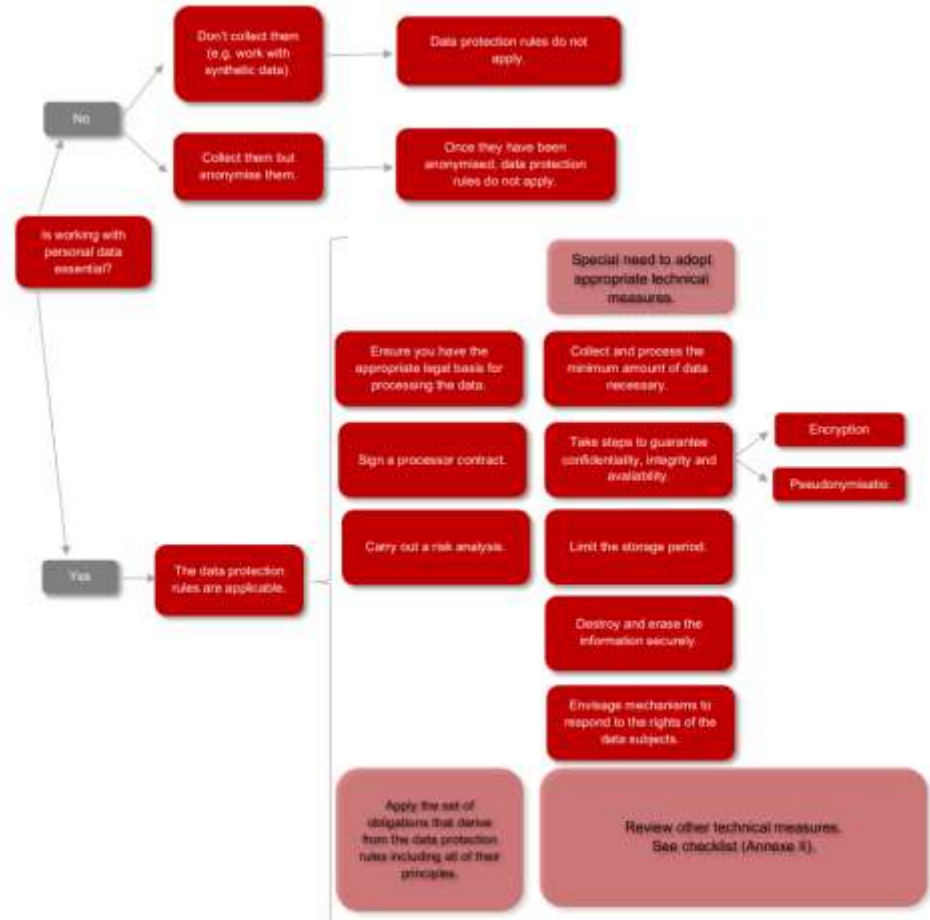


## Privacy by design and privacy by default

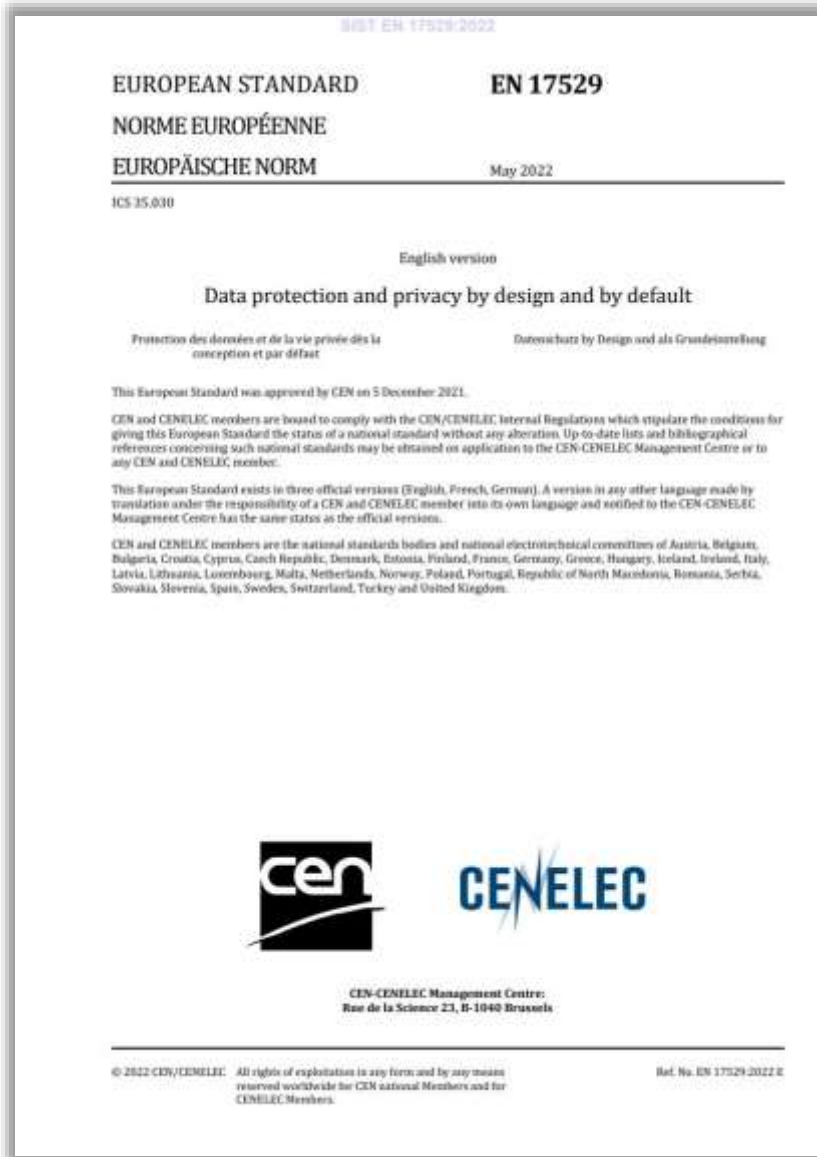
### A guide for developers

February 2023

Guides collection. No. 7

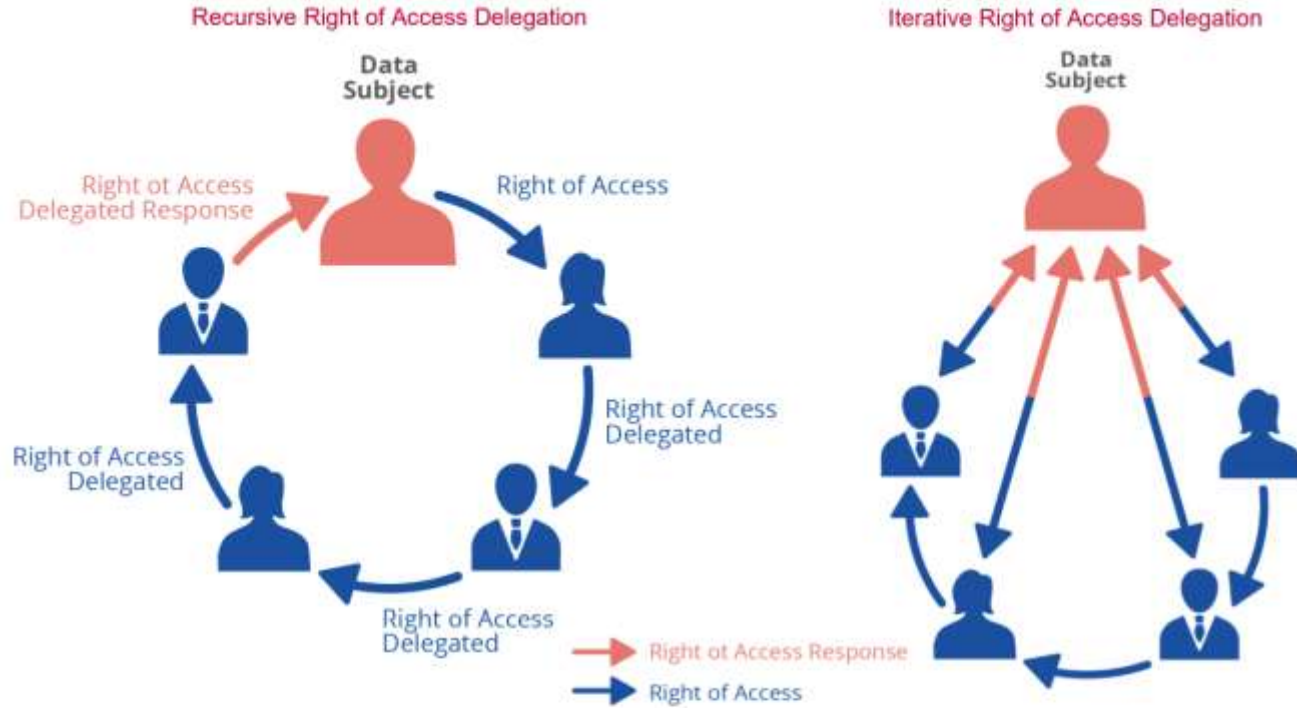


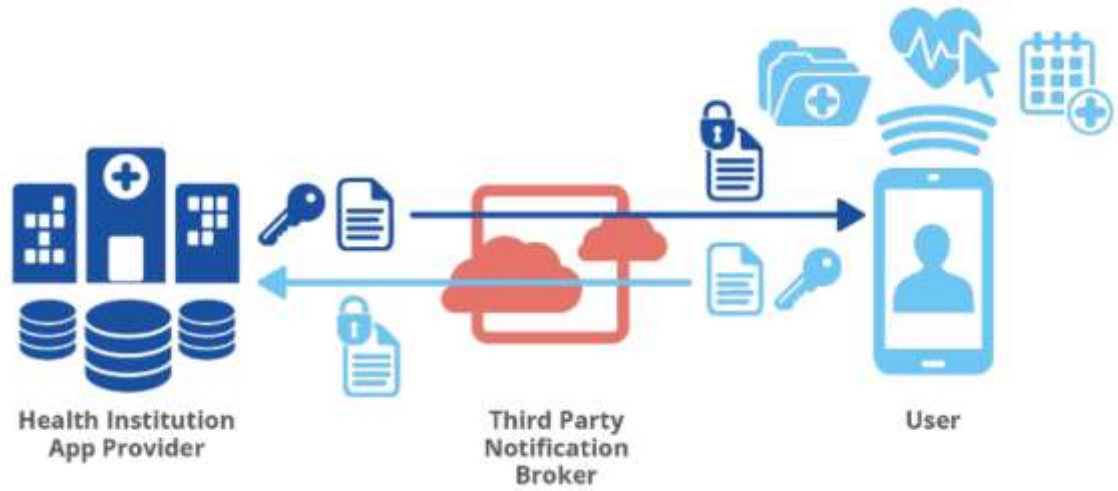
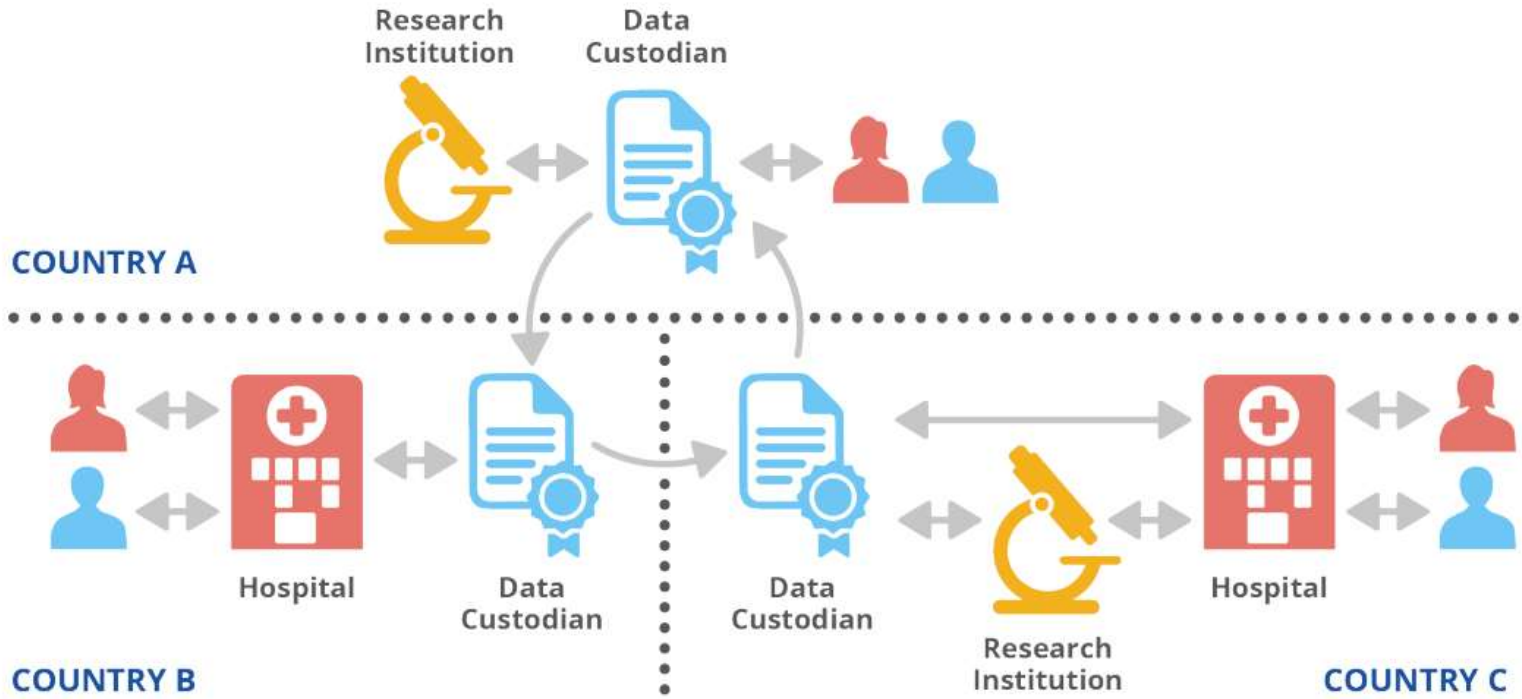
## 132 Стандарт EN 17529:2022. Data protection and Privacy by Design and by Default

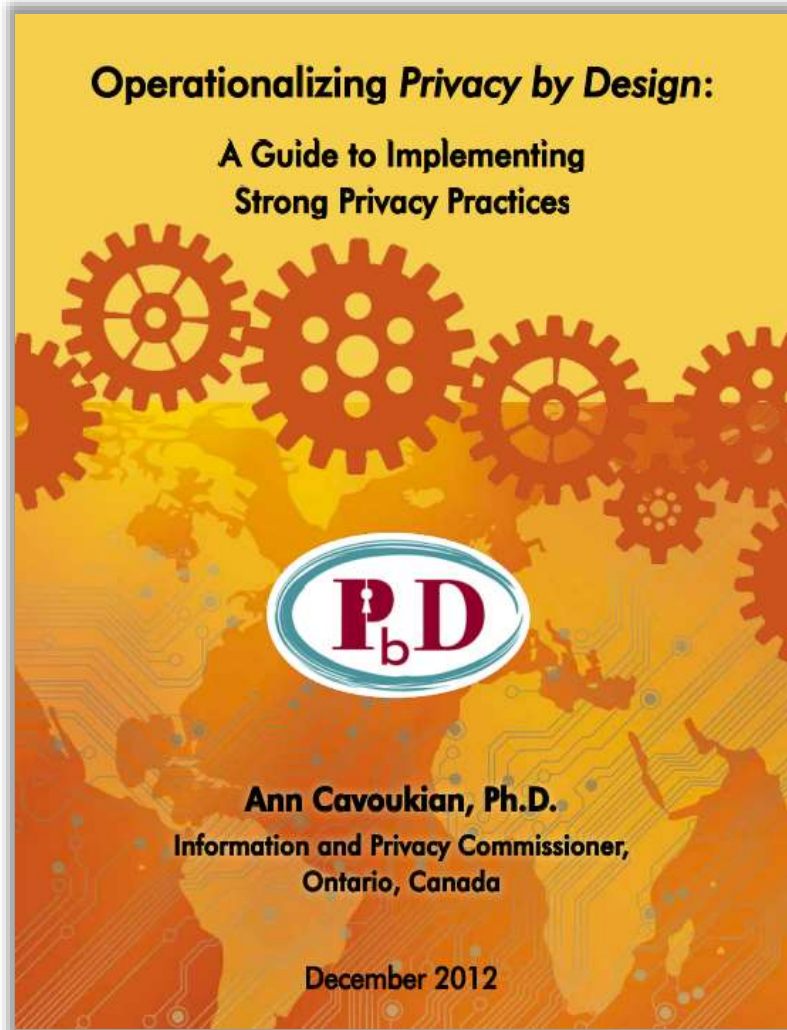


Европейский комитет по стандартизации CEN опубликовал стандарт EN 17529:2022 «Data protection and privacy by design and by default».

В документе содержатся требования к производителям и/или поставщикам услуг по внедрению методологии проектируемой и по умолчанию защиты персональных данных и неприкосновенности частной жизни (Data protection and Privacy by Design and by Default, DPbDD) на ранних этапах разработки своих продуктов и услуг, т. е. до (или независимо от) какой-либо конкретной интеграции приложений, с тем, чтобы обеспечить их максимальную готовность к обеспечению защиты неприкосновенности частной жизни (privacy ready). Документ применим ко всем секторам деловой деятельности, включая отрасль безопасности.







## The Fundamentals

Privacy: A Practical Definition

The 7 Foundational Principles of *Privacy by Design*

Implementation Guidance

## The 7 Foundational Principles of *Privacy by Design*

**Proactive** not Reactive; **Preventative** not Remedial

Privacy as the **Default Setting**

Privacy **Embedded** into Design

Full Functionality – **Positive-Sum**, not Zero-Sum

End-to-End Security – **Full Lifecycle Protection**

**Visibility** and **Transparency** – Keep it **Open**

**Respect** for User Privacy – Keep it **User-Centric**

## *Privacy by Design* Papers Organized by Application Area

CCTV/Surveillance Cameras in Mass Transit Systems:

Biometrics Used in Casinos and Gaming Facilities

Smart Meters and the Smart Grid

Mobile Devices & Communications

Near Field Communications (NFC)

RFIDs and Sensor Technologies

Redesigning IP Geolocation Data

Remote Home Health Care

Big Data and Data Analytics

Foundational *PbD* Papers

## *Privacy by Design* Papers Organized by Principle

1. **Proactive** not Reactive; **Preventative** not Remedial

2. Privacy as the **Default Setting**

3. Privacy **Embedded** into Design

4. Full Functionality – **Positive-Sum**, not Zero-Sum

5. End-to-End Security – **Full Lifecycle Protection**

6. **Visibility** and **Transparency** – Keep it **Open**

7. **Respect** for the User – Keep it **User-Centric**

The screenshot shows the ICO website header with the logo and tagline 'The ICO exists to empower you through information.' Below the header is a navigation menu with options: Home, For the public, For organisations (highlighted), Make a complaint, and Action we've taken. The breadcrumb trail reads: 'For organisations / UK GDPR guidance and resources / Data sharing / Privacy-enhancing technologies / What PETs are there?'. The main heading is 'What PETs are there?'. Below it is a list of bullet points describing various PETs.

**ico.**  
Information Commissioner's Office

The ICO exists to empower you through information.

Home For the public **For organisations** Make a complaint Action we've taken

For organisations / UK GDPR guidance and resources / Data sharing / Privacy-enhancing technologies / What PETs are there?

## What PETs are there?

- PETs are available for a variety of purposes (eg secure training of AI models, generating anonymous statistics and sharing information between different parties).
- Differential privacy generates anonymous statistics. This is usually done by randomising the computation process that adds noise to the output.
- Synthetic data provides realistic datasets in environments where access to large real datasets is not possible.
- Homomorphic encryption provides strong security and confidentiality by enabling computations on encrypted data without first decrypting it.
- Zero-knowledge proofs (ZKP) provide data minimisation by enabling someone to prove private information about themselves without revealing what it actually is.
- Trusted execution environments enhance security by enabling processing by a secure part of a computer processor that is isolated from the main operating system and other applications.
- Secure multiparty computation (SMPC) provides data minimisation and security by allowing different parties to jointly perform processing on their combined information, without any party needing to share all of its information with each of the other parties.
- Federated learning trains machine learning models in distributed settings while minimising the amount of personal information shared with each party. Using federated learning alone may not achieve appropriate protection of personal information. It may also require specific expertise to design mitigations (eg by combining with other PETs at different stages of your processing).

◇ Британское Управление комиссара по информации (ICO) опубликовало новое руководство по технологиям, улучшающим конфиденциальность (PETs). Руководство предназначено для DPO и других лиц, управляющих обработкой значительным количеством персональных данных в финансовой сфере, здравоохранении, научных исследованиях, центральных и местных органах власти.

◇ Первая часть руководства посвящена тому, как PETs могут помочь достичь соответствия закону о защите данных, а вторая часть имеет более технический подход и содержит более подробную информацию о типах PET, доступных в настоящее время.



## Заметка испанского AEPD про пространства данных, суверенитет данных и Privacy by Design



The screenshot shows the website of the Agencia Española de Protección de Datos (AEPD). The page features a search bar, navigation menu, and a main article titled "Data Spaces, sovereignty and privacy by design" dated 28 de September de 2023. The article text discusses Privacy Enhancing Technologies (PETs) and their role in implementing privacy principles within Data Spaces. A network diagram is included, and the article is attributed to Unsplash.

**Data Spaces, sovereignty and privacy by design**

28 de September de 2023

The Privacy Enhancing Technologies or PETs allow to implement the privacy principles, but the same tools are useful to implement the governance policies that guarantee the trust and data sovereignty in a Data Space.





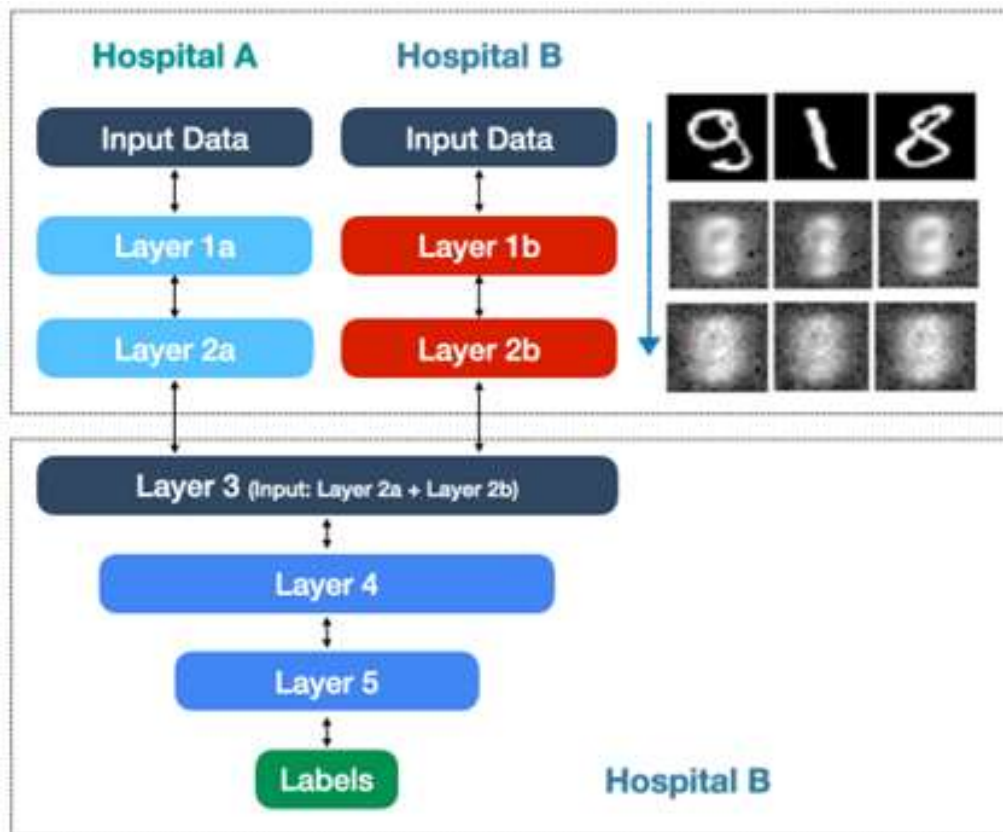
Unsplash

Data protection policies, like data protection by design and by default, mean the implementation management, legal and technical tools that guarantee compliance with GDPR. They should be devised in the early stages of the design of a Data Space. The Privacy Enhancing Technologies or PETs allow to implement the privacy principles, but the same tools are useful to implement the governance policies that guarantee the trust and data sovereignty in a Data Space. Therefore, PETs can be, and should be, "dual-use" technologies to be efficient and effective, integrated in the core of the Data Spaces, fulfilling different purposes in the data-access sharing economy.

Испанский орган по защите информации (AEPD) 28.09.2023 опубликовал заметку, посвященную технологиям, повышающим конфиденциальность (PETs). В частности, политики защиты данных, такие как Privacy By Design и By Default, предполагают применение управленческих, правовых и технических инструментов. PETs могут помочь в реализации принципов конфиденциальности и политики управления, обеспечивающих суверенитет данных. Эффективный суверенитет данных означает реализацию открытой и федеративной инфраструктуры, основанной на политике управления, правилах и стандартах, которые позволяют доверять всем заинтересованным сторонам путем эффективного доверия к их информационным активам. Такая безопасная среда обработки может создавать "пространство данных" с помощью таких инструментов и методов, как анонимизация/псевдонимизация, минимизация данных и использование синтетических данных.

Кроме того, в блоге говорится о том, что PETs могут реализовывать несколько вариантов использования, и в качестве примера приводятся средства отслеживания, которые используются, в частности, для монетизации данных, контроля интеллектуальной собственности и биллинговых процессов.

## 138 Испанский AEPD об объединенном обучении как методе PETs



Испанский орган по защите данных ('AEPD') опубликовал 26.04.2023 сообщение о методах объединенного обучения и соблюдении требований защиты данных и конфиденциальности. В частности, в блоге указано, что технологии объединенного обучения ('federated learning techniques') относятся к технологиям, повышающим конфиденциальность ('PETs'), и позволяют разрабатывать системы машинного обучения ('ML') без необходимости передачи персональных данных между участниками.

## 139 Заметка испанского AEPD про синтетические данные

◇ Испанский орган по защите информации (AEPD) 02.11.2023 опубликовал заметку, посвященную синтетическим данным и защите информации. Синтетические данные - это искусственно созданные данные, используемые при разработке, тестировании и проверке сервисов машинного обучения, в частности, когда реальных данных недостаточно или они недоступны.

◇ Синтетические данные потенциально могут облегчить доступ к информации как государственных, так и частных организаций, называемых пространствами данных, и тем самым способствовать развитию экономики, основанной на данных. Однако организации могут не решаться делиться данными, которые могут раскрыть коммерческие тайны, уязвимости или интеллектуальную собственность, не имея достаточных гарантий относительно целей и ограничений обработки данных, а также потенциального влияния на их интересы.

◇ Синтетические данные, как и другие технологии, могут выступать в качестве технологии повышения конфиденциальности (PET), поскольку позволяют применять принцип проектируемой защиты персональных данных (data protection by design) при разработке сценариев использования, требующих обработки персональных данных. В таких случаях генерация синтетических данных позволяет организациям минимизировать или избежать обработки персональных данных, достигая при этом поставленных целей с выводами, не уступающими тем, которые были получены при использовании исходных персональных данных.

◇ В соответствии с GDPR, синтетические данные не должны содержать идентифицирующей информации, даже если они могут быть созданы на основе реальных персональных данных. Поскольку синтетические данные сохраняют статистические свойства или распределение реальных персональных данных для определенной цели, такие данные могут быть использованы для минимизации обработки исходных персональных данных.

**Centre for Data Ethics and Innovation**  
PETs Adoption Guide  
BETA

Home

**BACKGROUND**

What are PETs?

Opportunities

**ADOPTING PETS**

PETs Adoption Guide

Repository of Use Cases

**FURTHER INFORMATION**

Good practice for sharing and processing data

Additional Resources

Contact us

Acknowledgements

## Examples of traditional PETs

- > Encryption in transit and at rest
- > De-Identification Techniques

## Examples of emerging PETs

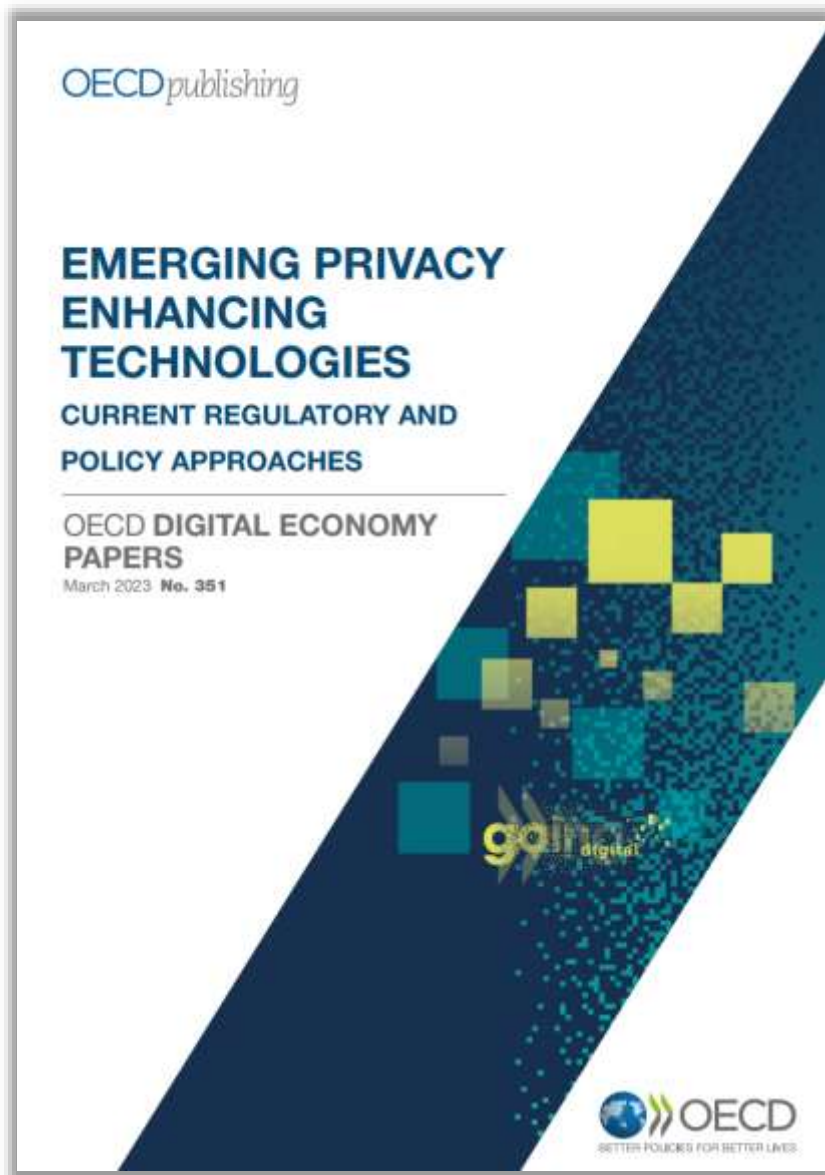
- > Homomorphic encryption
- > Trusted Execution Environments
- > Multi-party computation
- > Differential Privacy
- > Federated Analytics

# Белая книга CIPL о роли PETs (Privacy-Enhancing Technologies) и PPTs (Privacy-Preserving Technologies) в цифровую эпоху



PET	Use	Data Protection Principles Supported	Key Benefits	Limitations	Solutions
Homomorphic encryption	Perform computations on encrypted data without revealing data	Provides secure data processing May have potential to anonymize data, removing the need to comply with personal data protection requirements and restrictions	Secure data sharing and collaboration Secure outsourcing of computations or processing to third parties Reduces the risk of data leaks as data remains hidden	High computing resources required during encryption and processing for specific types of data and computations Complexity	Algorithmic and hardware improvements improve overall performance Open-source compilers and libraries are making it easier to use and implement, as well as vendors that provide solutions that already incorporate homomorphic encryption
Secure multi-party computation	Allows computation on data held across multiple parties without revealing or transferring any data beyond the results of the computation	Can support the data minimization principle Provides secure data processing Avoids the restrictions on data sharing	Secure data sharing and collaboration	Communications between parties may allow data to be reconstructed High communication costs, leading to scalability issues Complexity	The use of auditing and accountability measures or other PETs, such as homomorphic encryption, can help address the risk of collusion between parties Advances in protocol design and techniques Easy-to-use compilers and libraries are available
Trusted execution environments	Keep data and code secure during use	Provides secure data processing Supports the purpose limitation principle	Provides high level protection against attackers	Security (side-channel attacks) Trust Speed Lack of standards	Addressing side-channel attacks is difficult, but this technology can act as a great security layer and should be used in combination with other PETs to maximize security Attestation mechanisms Cloud computing can offer greater computing resources Project communities are bringing together different stakeholders to accelerate the adoption of technologies and standards
Zero-knowledge proofs	Verify knowledge without revealing the data necessary to prove it	Supports the data minimization principle	Secure data sharing by proving certain properties of the data	Performance overhead on the parties generating and verifying the proofs Security Lack of standards	More efficient zero-knowledge proofs are being developed, and computational power is continuously increasing over time Some zero-knowledge proofs require a trusted setup process which must be carefully implemented Initiatives are bringing together different stakeholders to develop standards and best practices

## Отчет от ОЭСР по глобальным практикам использования технологий усиления приватности (PETs) в 2023 году



В отчете рассматриваются последние технологические достижения и оценивается эффективность различных типов PETs, а также проблемы и возможности, которые они представляют. В нем также описываются существующие подходы к PETs в области регулирования и политики, чтобы помочь органам по обеспечению соблюдения конфиденциальности и разработчикам политики лучше понять, как их можно использовать для повышения конфиденциальности и защиты данных, а также для улучшения общего управления данными.

### 1 Introduction

- 1.1. The emergence of privacy-enhancing technologies
- 1.2. Goals of the report
- 1.3. Evolving paradigms
- 1.4. Moving towards privacy and data protection by design

### 2 Current definitions and categorisations of PETs

- 2.1. Towards a common understanding of privacy-enhancing technologies
- 2.2. Existing definitions and their evolution
- 2.3. Existing categorisations
- 2.4. Proposed working definition and taxonomy

### 3 Major types of PETs, their maturity, opportunities and challenges

- 3.1 Categories of privacy-enhancing technologies (PETs)
- 3.2. Data obfuscation tools
- 3.3. Encrypted data processing tools
- 3.4. Federated and distributed analytics
- 3.5. Data accountability tools

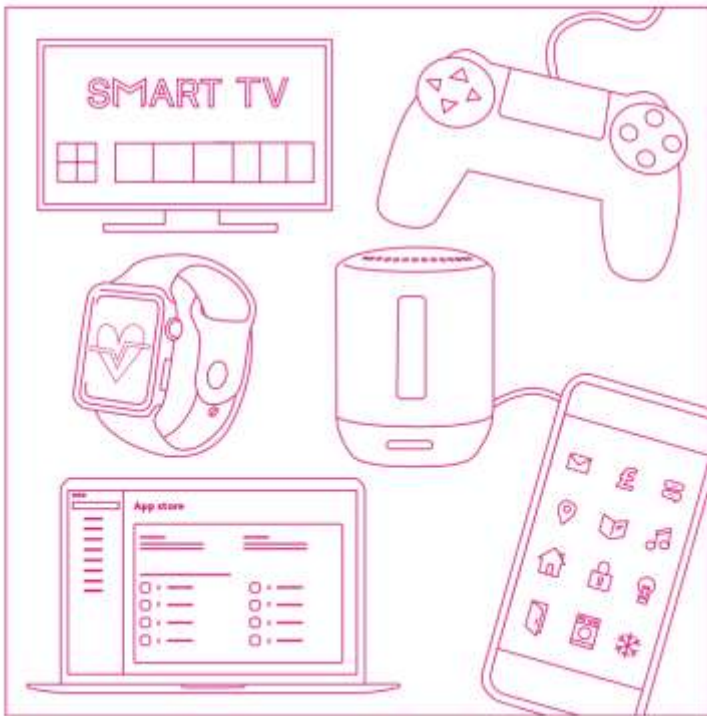
### 4 Regulatory and policy approaches to PETs

- 4.1. Legislation and guidance on the use of PETs
- 4.2. Measures to foster innovation in and with PETs

## Кодекс практики для операторов и разработчиков магазинов приложений от британского DCMS



### Code of Practice for App Store Operators and App Developers



Британское министерство цифровых технологий, культуры, СМИ и спорта ("DCMS") опубликовало 09.12.2022 Кодекс практики для операторов и разработчиков магазинов приложений. Кодекс практики является добровольным и включает новые меры, такие как предоставление информации о безопасности и конфиденциальности пользователям в ясной и простой для понимания форме. Кодекс предусматривает, что операторы магазинов приложений и разработчики должны предоставлять потребителям информацию о безопасности и конфиденциальности в удобном для пользователя виде, опубликованную в месте, не требующем покупки разработчиками.

Кроме того, операторы магазинов приложений и разработчики должны разрешить работу своих приложений, даже если пользователь решит отключить дополнительные функции и разрешения, например, запретить приложению доступ к микрофону или знать местоположение пользователя.

### Protection against Tracking

This pattern avoids the tracking of visitors of websites via cookies. It does this by deleting them at regular intervals or by disabling cookies completely.

### Minimal Information Asymmetry

Prevent users from being disenfranchised by their lack of familiarity with the policies, potential risks, and their agency within processing.

### Awareness Feed

Users need to be informed about how visible data about them is, and what may be derived from that data. This allows them to reconsider what they are comfortable about sharing, and take action if desired.

### Location Granularity

Support minimization of data collection and distribution. Important when a service is collecting location data from or about a user, or transmitting location data about a user to a third-party.

### Informed Secure Passwords

Ensure that users maintain healthy authentication habits through awareness and understanding.

### Encryption with user-managed keys

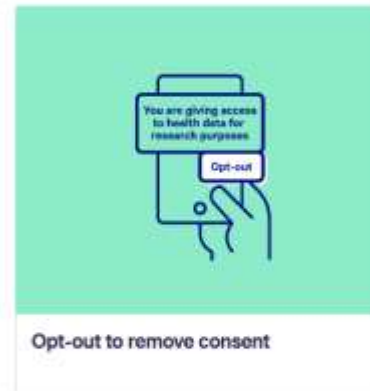
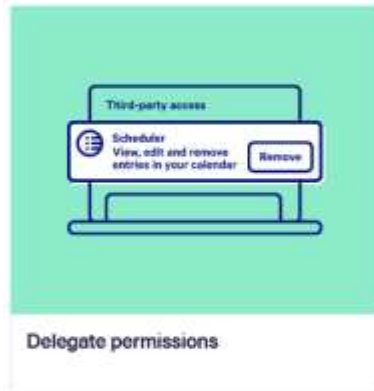
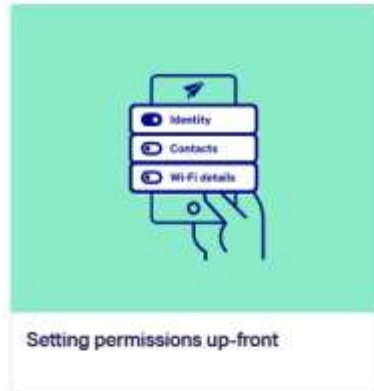
Use encryption in such a way that the service provider cannot decrypt the user's information because the user manages the keys.

### Categories

- +  CONTROL
- +  ABSTRACT
- +  SEPARATE
- +  HIDE
- +  MINIMIZE
- +  INFORM
- +  ENFORCE



## 145 База с паттернами Privacy by Design по предоставлению и отзыву согласий



I. PREREQUISITES	
A. PRIVACY GOVERNANCE	B. RISK MODEL
Evidence And Evaluation	Evidence And Evaluation

Prerequisites are organizational Components that do not relate, specifically, to the design process. Each prerequisite has its own Evidence and Evaluation requirements.

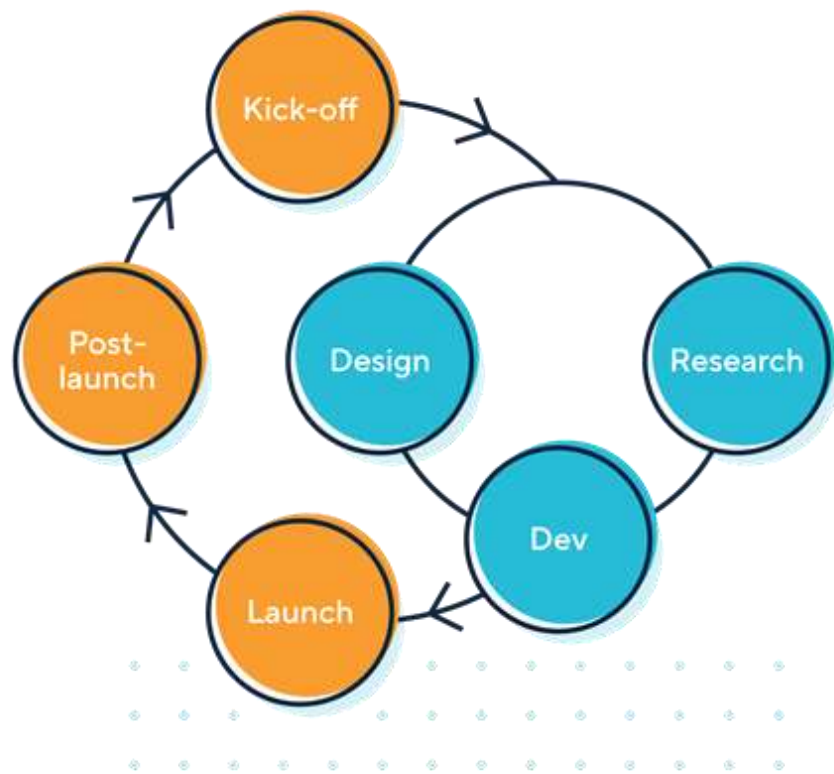


All of the Design Process Components are aligned with one or more of the stages of the product, service or business process lifecycle. The stages are presented at a very high level to avoid conflict with organizations that may have more granular stages.

a. Contextualize risk factors	E & E
b. Elicit privacy issues	E & E
c. Assess risks	E & E
2. RESPOND TO RISKS	
Evidence And Evaluation	

All Design Process Components have Evidence and Evaluation requirements beyond the general Evidence and Evaluation requirements for the entire design process. The Manage Privacy Risks Component is divided into two sub-components, the first of which is further subdivided. Each of the subcomponents has Evidence and Evaluation requirements.

## Рекомендации британского ICO по обеспечению приватности в жизненном цикле разработки продукта



**The case for privacy** – Your organisation must comply with relevant laws. But there are also pressing reasons beyond legal compliance to prioritise privacy. For example, the risk of harming people and society itself, as well as the business risks to organisations.

**Privacy in the kick-off stage** – including kick-starting collaboration, mapping your product’s personal information needs, and ideas on weaving privacy into your business case.

**Privacy in the research stage** – including gathering up-front perspectives on privacy, testing of work in progress, and ways to protect the personal information of research participants.

**Privacy in the design stage** – including choosing the right moments, obtaining valid consent, and communicating privacy information in ways people understand.

**Privacy in the development stage** – including defining the appropriate amount of personal information required, exploring technical solutions that enhance privacy, and protecting personal information in development environments.

**Privacy in the launch phase** – including conducting pre-release checks, factoring privacy into rollout plans, and deciding how best to communicate changes.

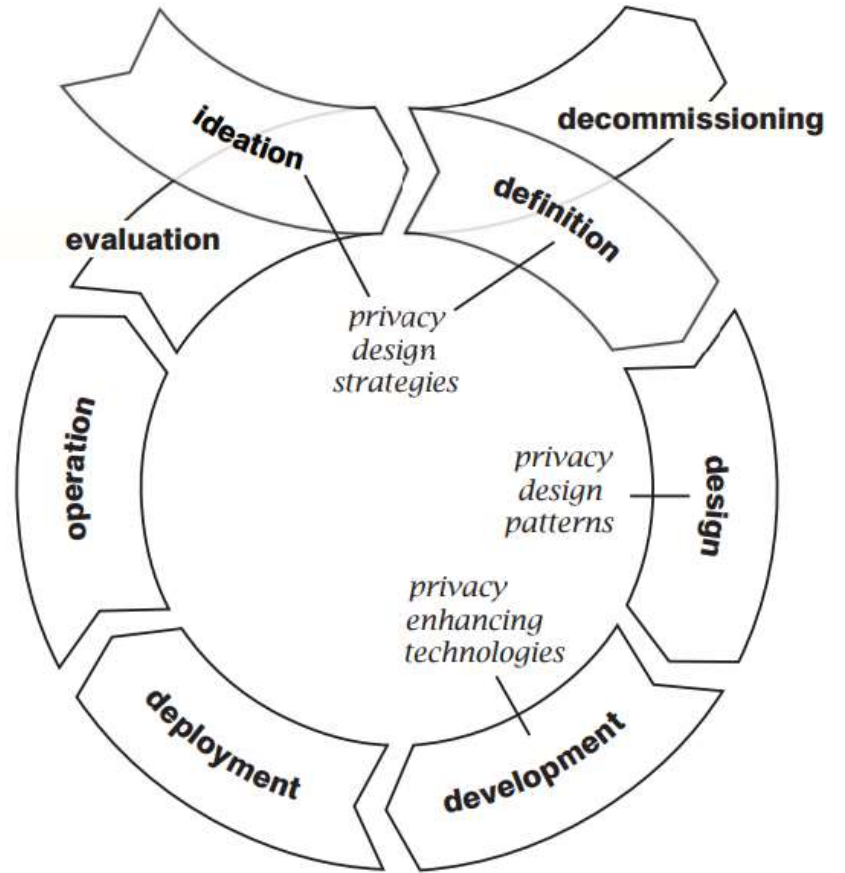
**Privacy in the post-launch phase** – including monitoring and triaging fixes, reappraising expectations and norms, and celebrating privacy successes.

Privacy Design Strategies  
(The Little Blue Book)

The diagram illustrates the relationship between a Data subject and a Data controller. At the top, a box labeled 'Data subject' has an upward arrow from an 'inform' icon (an 'i' in a circle) and a downward arrow to a 'control' icon (a game controller). Below this, a larger box labeled 'Data controller' contains several icons: a 'separate' icon (two arrows pointing away from each other), a 'minimise' icon (a pair of scissors), an 'abstract' icon (a magnifying glass over a minus sign), a 'hide' icon (an eye with a slash through it), a 'demonstrate' icon (a document with a checkmark), and an 'enforce' icon (a shield). The entire diagram is set against a blue background.

Jaap-Henk Hoepman

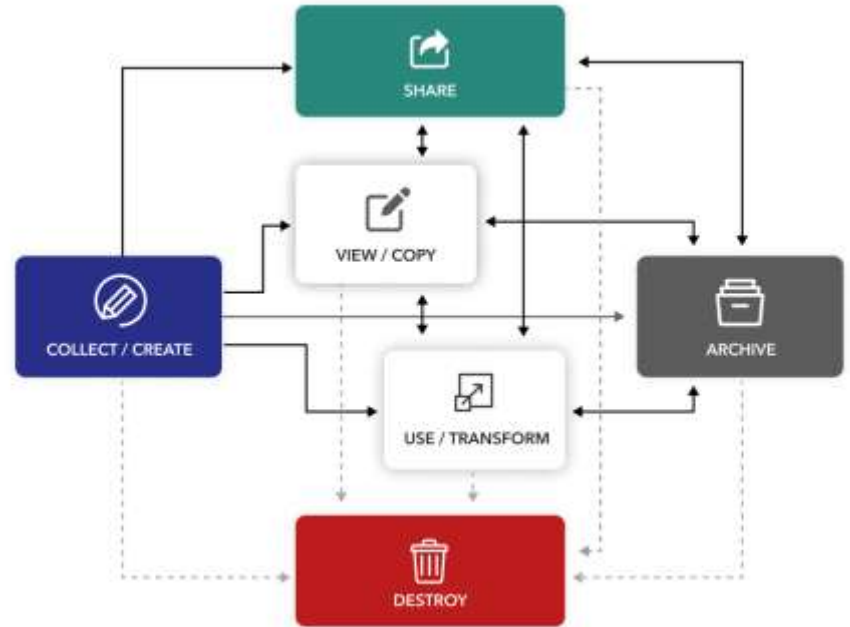
April 19, 2022





# Privacy By Design: From Principles to Requirements

Mark Settle



1. Full Lifecycle Protection
2. Maximum Use of Embedded Safeguards
3. Exposure Based on Least Need
4. Shared Management of Personally Identifiable Information
5. Proactive Privacy Assurance



<b>Background and Overview</b>	<b>2</b>
<b>1. THE FUNDAMENTALS OF DATA PROTECTION BY DESIGN AND BY DEFAULT IN THE GDPR</b>	<b>4</b>
1.1. Origins and status of Data Protection by Design and by Default, from broad policy goal to legal obligation under the GDPR	5
1.2. Perceived limitations of Article 25 GDPR: vague wording, limited personal scope	6
1.3. Privacy Enhancing Technologies (PETs) support DPbD&bD, but they are not always sufficient to comply with Article 25 GDPR	6
<b>2. UNDERSTANDING TRENDS IN THE ENFORCEMENT OF DATA PROTECTION BY DESIGN AND BY DEFAULT OBLIGATIONS</b>	<b>8</b>
2.1. First steps in assessing Article 25 compliance: context of processing, risks, and the TOMs appropriate to them	10
a. The controller is responsible to comply with the DPbD&bD obligations, but the relationship with processors is under increased scrutiny	10
b. The DPbD&bD obligations are context-dependent, weighing in the state-of-the-art of technology, the cost of implementation, the nature of the processing, and the likelihood of risks	12
c. TOMs must be comprehensive: organizational measures, like training and frequent vulnerability tests, matter as much as technical measures, like encryption	15
d. TOMs must be in place before and during the processing	17
e. TOMs need to be effective in preventing the materialization of risks	18
2.2. Data protection principles and the rights of the data subject must be ensured "by design"	20
a. Controllers often jointly breach DPbD&bD and Article 5 principles, like data minimization	20
i. Lawfulness, Transparency, and Fairness	21
ii. Purpose Limitation	27
iii. Data Minimization	28
iv. Accuracy	31
v. Storage Limitation	33
vi. Integrity and Confidentiality	34
vii. Accountability	40
b. DPAs focus on data subjects' rights and freedoms enshrined in the GDPR	41
2.3. Data Protection by Default should prevent the manipulation of individuals online	43
2.4. Divergent practice emerges related to non-material damages for DPbD&bD breaches	47
<b>3. SPECIFIC SCENARIOS RELATED TO NEW TECHNOLOGIES: DIRECT MARKETING, PETS IN ONLINE ENVIRONMENTS, AND EDTECH</b>	<b>50</b>
3.1. Direct Marketing: lack of consent and the right to object as a DPbD&bD infringement	50
3.2. Privacy Preservation in Online Environments and the increasing role of PETs	54
3.3. EdTech: proctoring and virtual learning tools are subject to strict requirements	56
<b>4. CONCLUSION</b>	<b>59</b>
<b>Annex I — List of cases</b>	<b>63</b>
<b>Annex II — Comparative overview of DPA enforcement actions across the EEA</b>	<b>71</b>
<b>References</b>	<b>72</b>

## 151 **Awesome Privacy Engineering на GitHub**

- [Courses](#)
- [Books](#)
- [Data Deletion, Data Mapping, and Data Subject Access Requests](#)
- [Privacy Tech Series](#)
- [Privacy Threat Modeling](#)
- [Machine Learning and Algorithmic Bias](#)
- [Facial Recognition](#)
- [De-Identification and Anonymization](#)
- [Homomorphic Encryption](#)
- [Tokenization](#)
- [Secure Multi-Party Computation](#)
- [Synthetic Data](#)
- [Differential Privacy and Federated Learning](#)
- [Designing for Trust with Users](#)
- [Deceptive Design Patterns](#)
- [Tagging Personally Identifiable Information](#)
- [Regulatory and Framework Resources](#)
- [Conferences](#)
- [Career](#)
- [Miscellaneous](#)
- [Other Awesome Privacy Curations](#)
- [Related Github Topics](#)

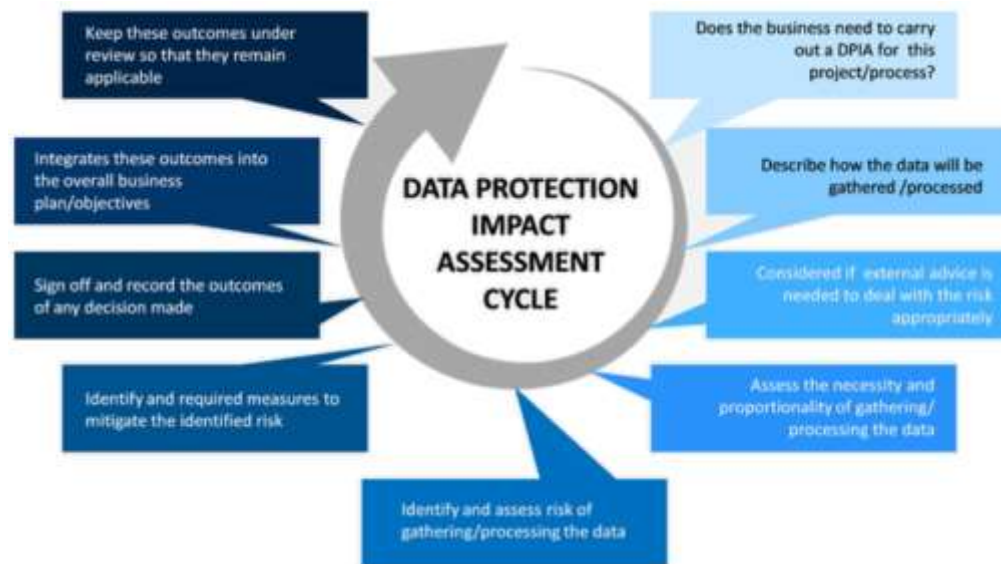
# Data Protection Impact Assessment



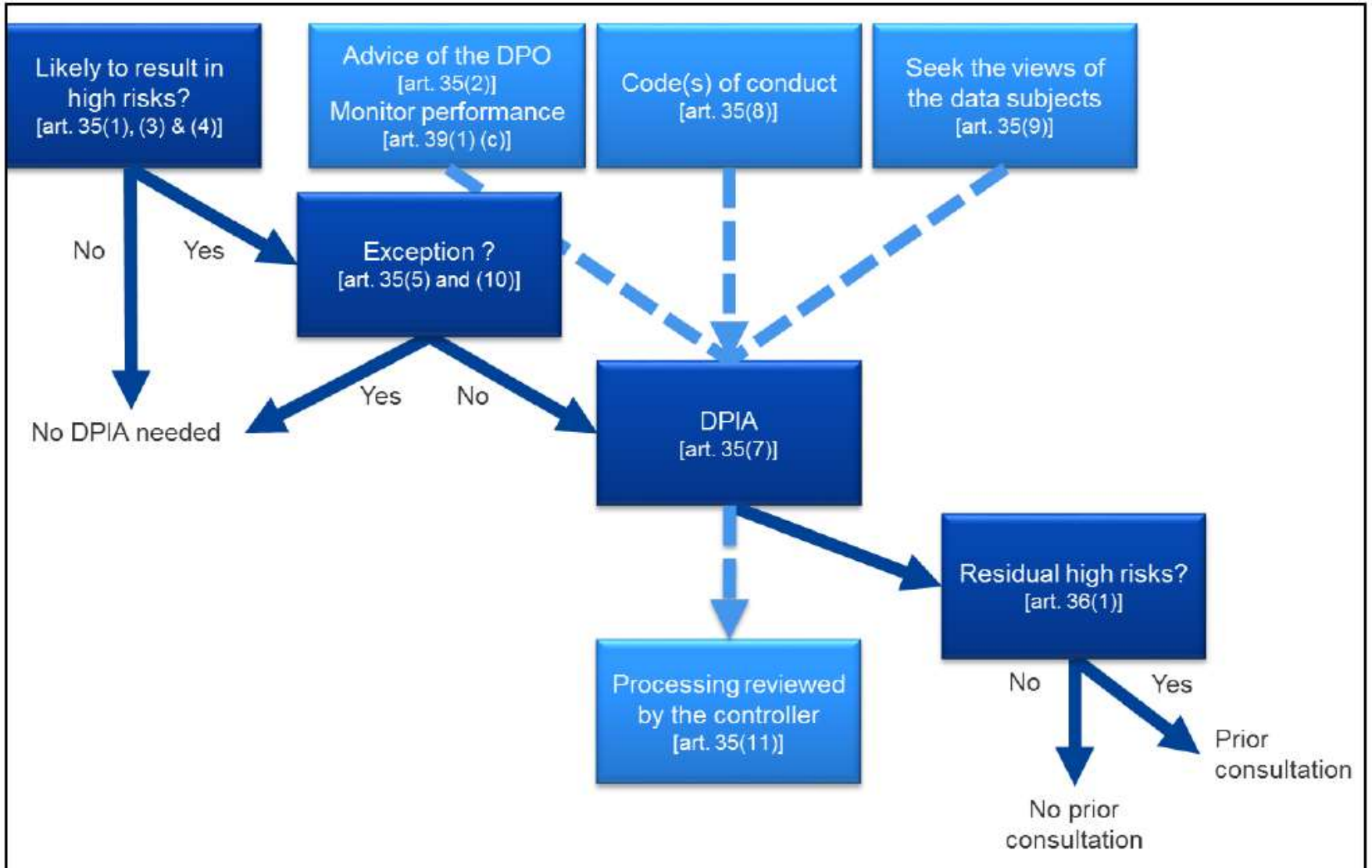


## 153 Data Protection Impact Assessment (DPIA)

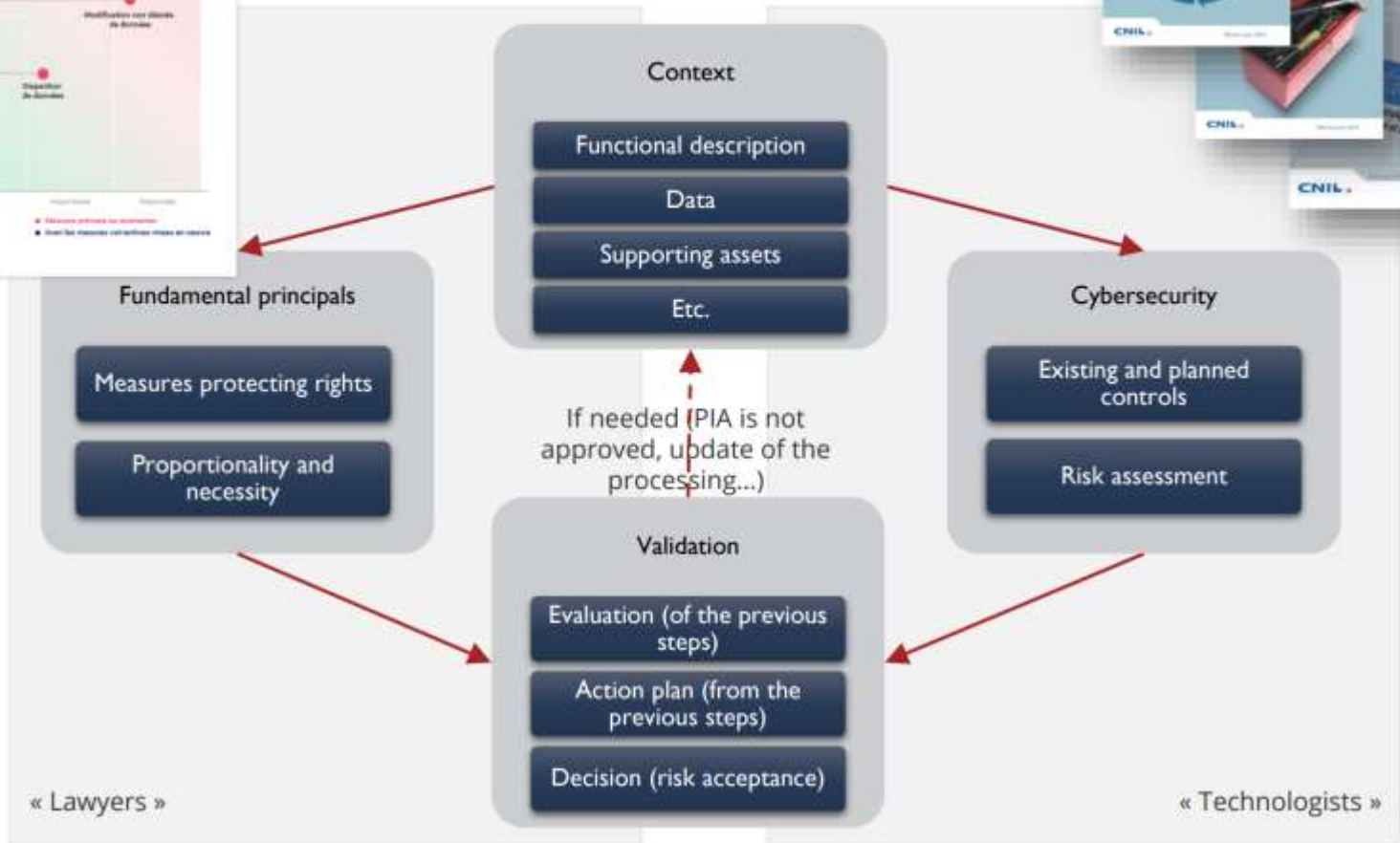
Оценка воздействия на защиту персональных данных (Data Protection Impact Assessment, DPIA) — процедура, предусмотренная ст. 35 Общего регламента защиты персональных данных ЕС (GDPR). Она заключается в выявлении и описании всех процессов работы с персональными данными внутри компании. DPIA проводится для оценки рисков негативного воздействия на данные, поиска наиболее уязвимых мест в системе защиты, но главное — для выработки действий по недопущению утечек и ошибок.



- ✓ Обязательно нужно проводить при скоринге, мониторинге, обработке больших объемов специальных категорий данных и при других аналогичных операциях с высоким риском для субъекта (передача данных за пределы ЕС, применение технических новшеств, обработка данных слабозащищённых лиц).
- ✓ Контролер так же должен провести процедуры оценки рисков, для выявления критичных процессов, для которых DPIA нужно провести дополнительно.
- ✓ Основная цель - понять последствия, которые могут наступить для субъекта и для контролера/процессора в случае, если что-то пойдет не так.
- ✓ GDPR ставит задачи, обязательно решаемые в ходе DPIA. Структуру, форму и методологию контролер/процессор определяет самостоятельно.
- ✓ Вопрос необходимости проведения DPIA рекомендуется внедрить в процессы Privacy by Design.
- **Важным аспектом для принятия решения о необходимости DPIA является качественная оценка рисков в процессах обработки персональных данных.**







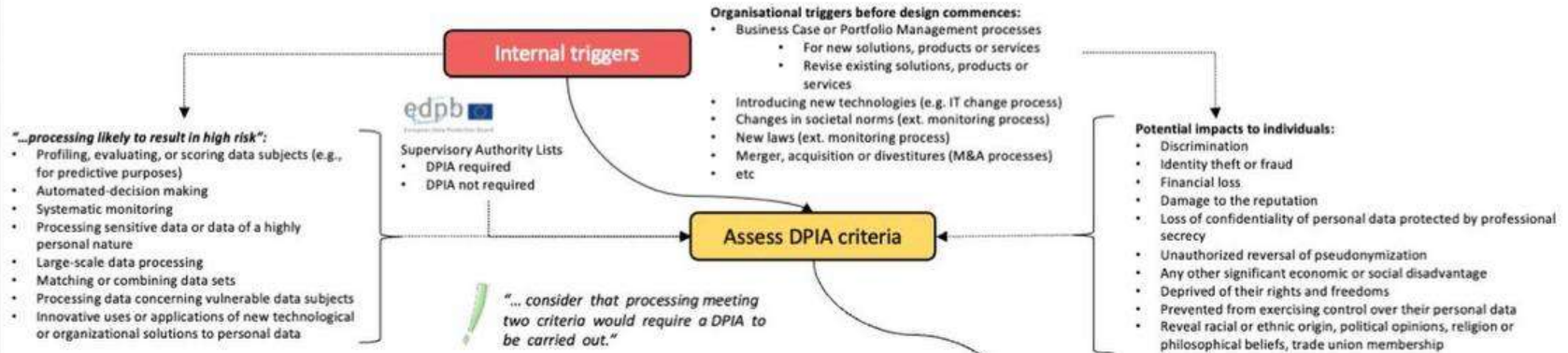
# DPIA ON A PAGE

## WHY?

DPIAs have two main values:

- To help identify and minimise data protection risks in your company's products, apps, solutions, etc that process data about people
- Demonstrating compliance to Supervisory Authorities

## WHEN?

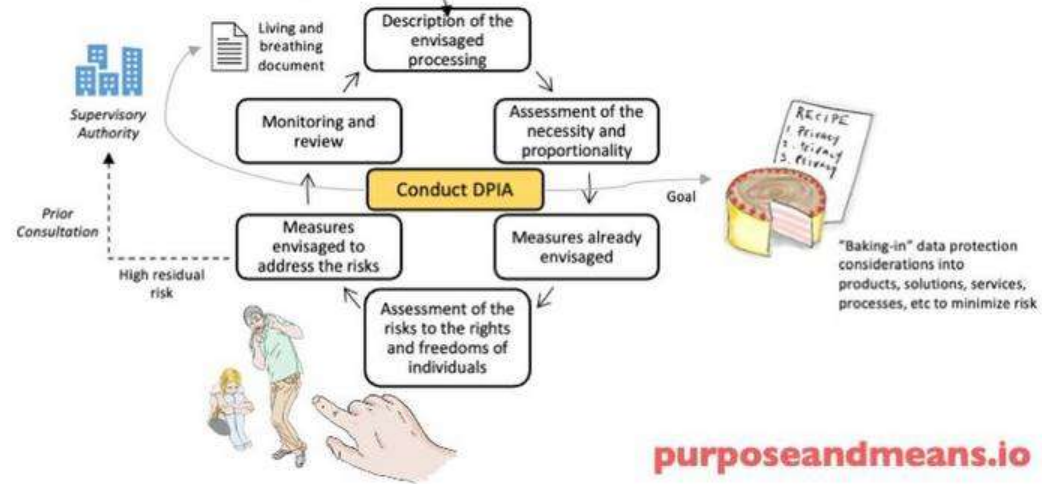


## WHO?

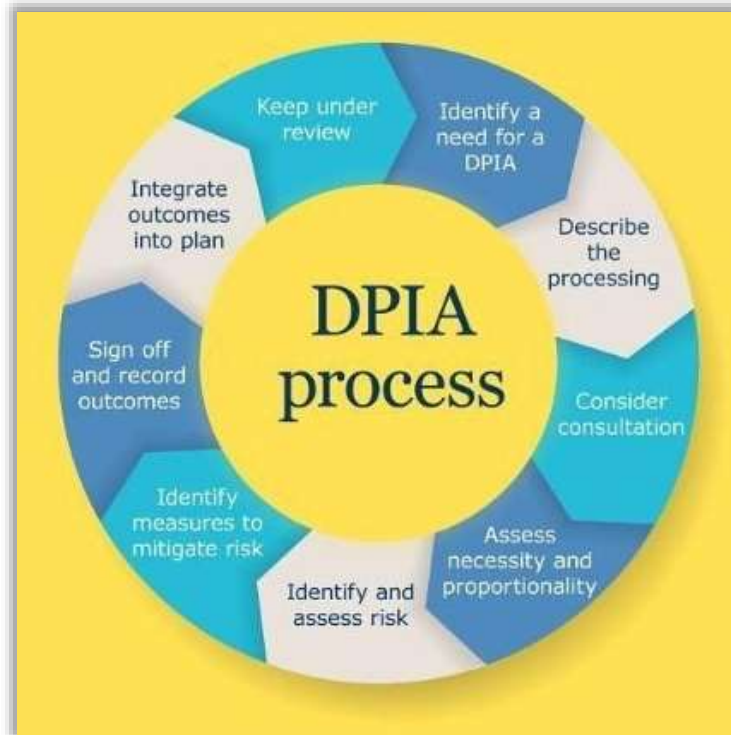
It's a collaborative effort



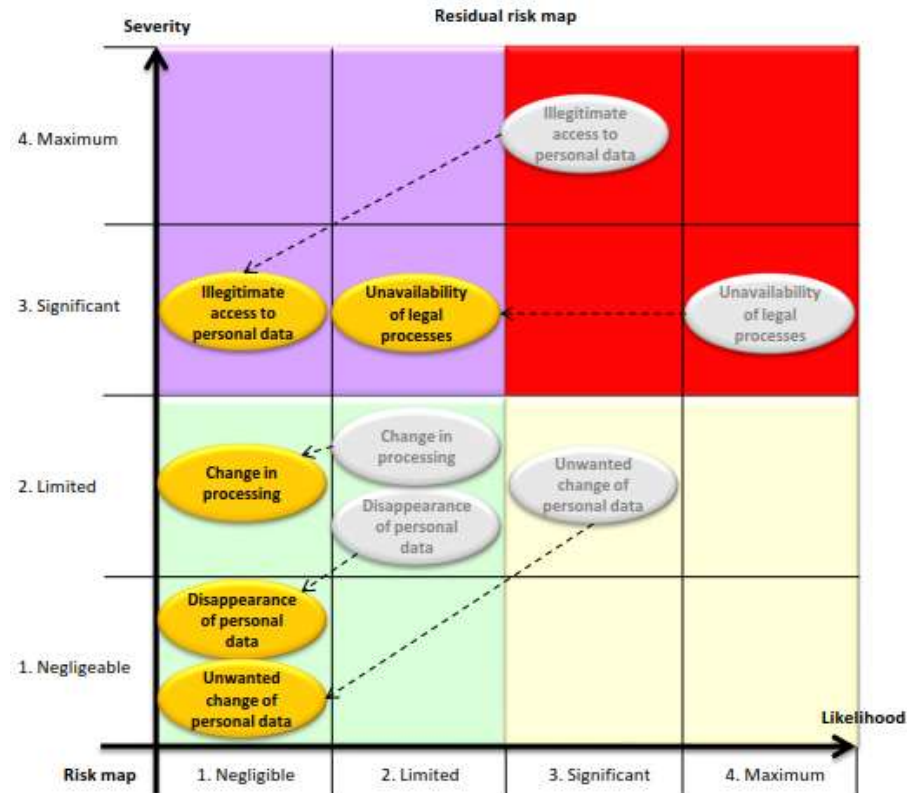
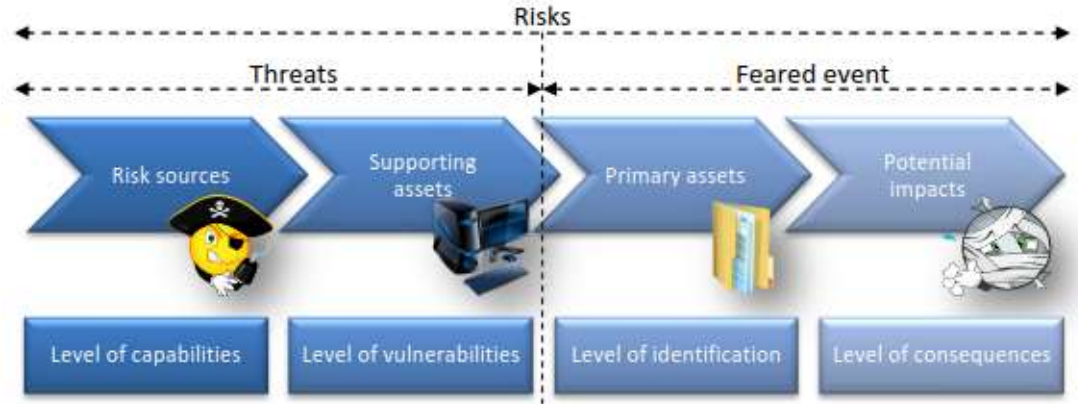
## HOW?



## Руководство ICO по проведению DPIA и типовой шаблон отчета о проведении DPIA



<b>Severity of impact</b>	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
<b>Likelihood of harm</b>				



## 160 Руководство CNIL по осуществлению Privacy Impact Assessment (PIA)



### GUIDELINES

#### PRIVACY IMPACT ASSESSMENT (PIA) : APPLICATION TO CONNECTED OBJECTS



### GUIDELINES

#### PRIVACY IMPACT ASSESSMENT (PIA) 1 : METHODOLOGY



### GUIDELINES

#### PRIVACY IMPACT ASSESSMENT (PIA) 2 : TEMPLATE



### GUIDELINES

#### PRIVACY IMPACT ASSESSMENT (PIA) 3 : KNOWLEDGE BASES



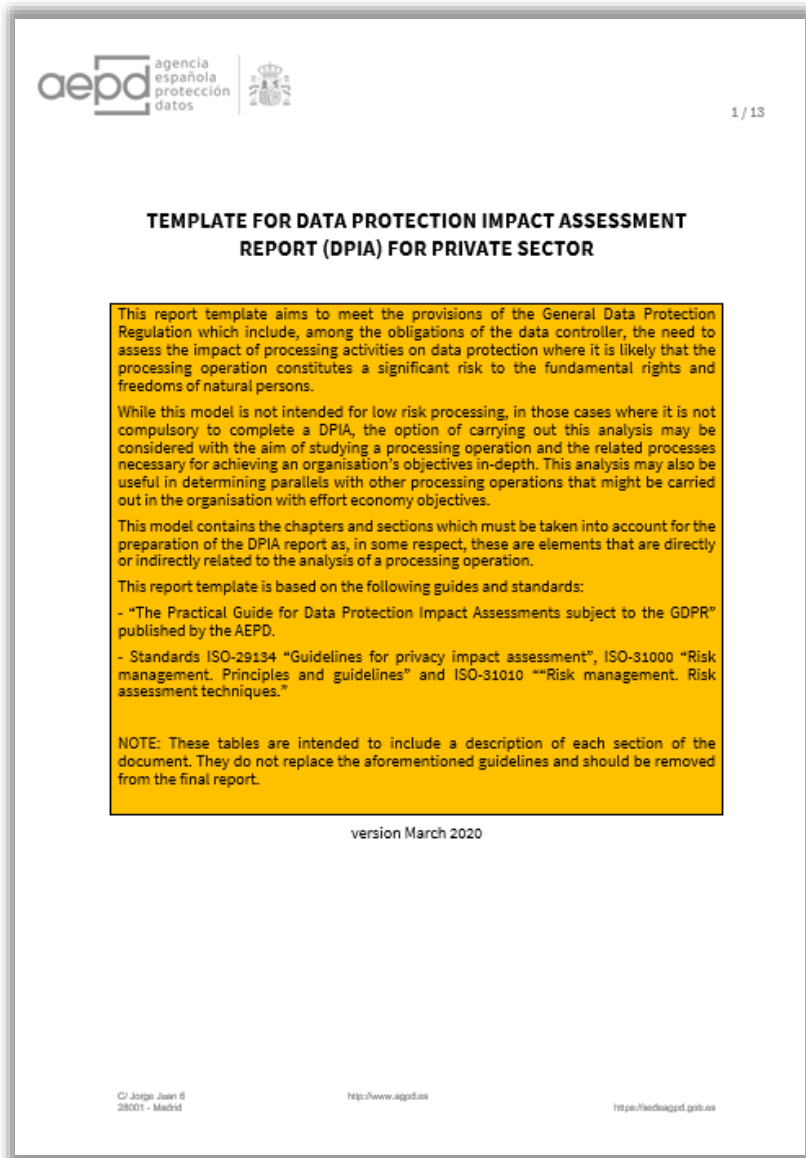
## 161 Рекомендации французского CNIL по высокорисковой обработке данных



Рекомендации применяются к процедурам обеспечения безопасности автоматизированной обработки персональных данных, представляющих высокий риск, так называемым "критическим операциям обработки". Такая обработка характеризуется:

- обработкой данных значительного масштаба; и
- возможным нарушением безопасности персональных данных, которое может привести к очень значительным последствиям для заинтересованных лиц, безопасности государства или общества в целом.

# 162 Пример реализации DPIA от AEPD для частного сектора



I. EXECUTIVE SUMMARY .....	
II. TABLE OF CONTENTS .....	
III. PURPOSE OF THE PROCESSING OPERATION .....	
Date of preparation of the DPIA .....	
Name and Description of Processor .....	
Categories of Data .....	
Identification of the Data Controller as per GDPR .....	
Identification of third parties involved in processing .....	
Internal context of the processing operation in the organisation .....	
External context of the organisation and the processing operation .....	
IV. LAWFULNESS OF PROCESSING AND REGULATORY COMPLIANCE .....	
V. DPIA METHODOLOGY .....	
Parties involved in the completion of the DPIA .....	
Guidelines, tools, methodologies, standards and rulings used in the evaluation .....	
Scope and limits of the DPIA: Identify what remains outside the scope of the assessment .....	
VI. ANALYSIS OF THE PROCESSING OPERATION .....	
VII. ANALYSIS OF THE OBLIGATION TO COMPLETE A DPIA: RISK ASSESSMENT .....	
Inclusion of processing operation in the list of exempt processing operations .....	
Analysis of obligation to complete DPIA for the processing operation .....	
Assessment of level of risk .....	
VIII. ANALYSIS OF THE NEED FOR THE PROCESSING OPERATION .....	
Benefits for data subjects .....	
Benefits for the entity .....	
Alternatives to the processing operation and why they were not chosen .....	
IX. MEASURES TO REDUCE THE RISK .....	
Optimising the processing operation .....	
Privacy by design and default (PBDD) measures .....	
Accountability measures .....	
Security Measures .....	
X. RISK-BENEFIT ANALYSIS .....	
XI. ACTION PLAN .....	
XII. CONCLUSIONS AND RECOMMENDATIONS .....	
XIII. APPENDICES .....	

<https://www.aepd.es/sites/default/files/2020-03/modelo-informe-EIPD-sector-privado-en.rtf>

<https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-nueva-guia-gestionar-riesgos-y-evaluaciones-impacto>

## 163 Веб-сервис «Gestiona» испанского AEPD для проведения DPIA

Веб-сервис предназначен для небольших государственных или частных организаций и позволяет управлять процедурами, осуществлять управление рисками и, при необходимости, оказывать поддержку в проведении оценки воздействия. Инструмент был переработан с более интуитивным дизайном и включает в себя последние рекомендации, содержащиеся в руководствах, опубликованных AEPD. Теперь появляется возможность комплексно вести RoPA организации, включая до 500 видов деятельности по обработке данных, в том числе вести RoPA и проводить DPIA различных организаций.

### New personal data processing

**Data processing Id**  
Name for identifying data processing (max 50 characters)

Data processing name

Short description

Data processing description

**Typical processing in SMEs**  
In case the entity is an SME, the following processing are pre-assessed. Please select the one to which this processing applies (only one):

**More...**

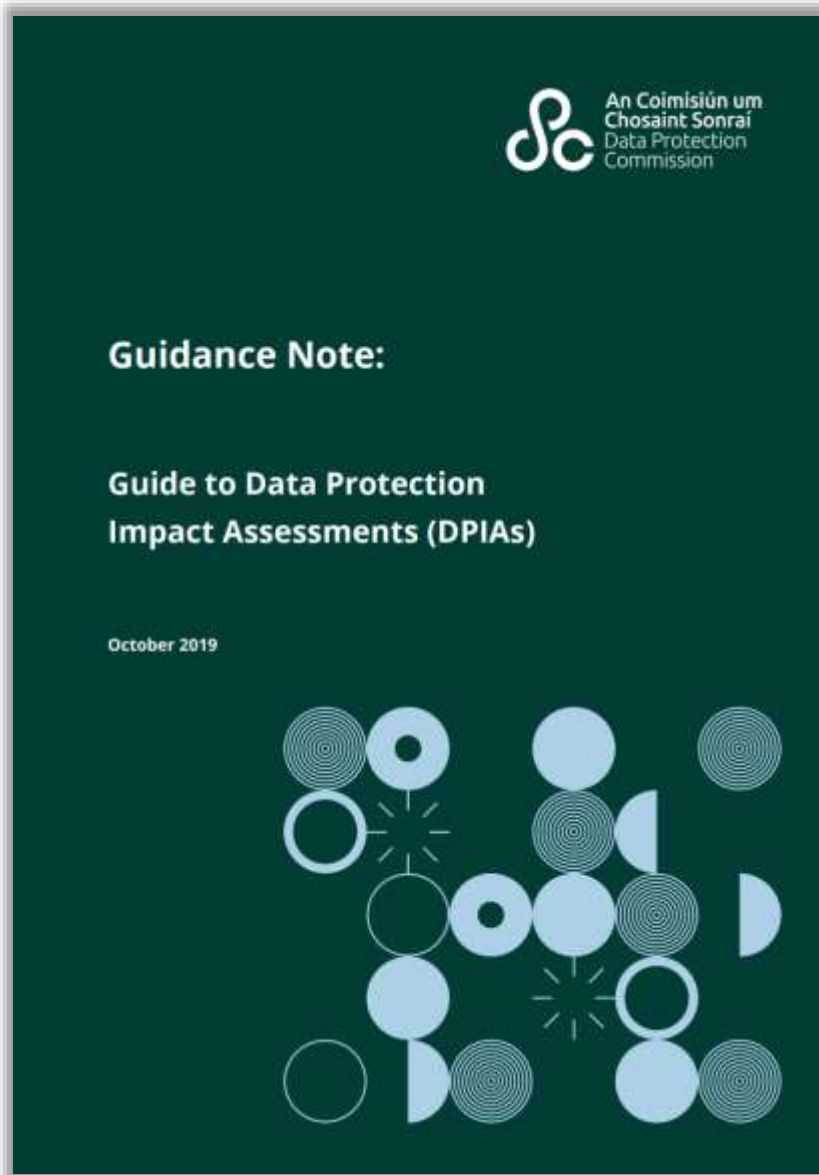
<input type="checkbox"/> Customer service	<input type="checkbox"/> Recruitment of new staff (HR)
<input type="checkbox"/> Actions to attract potential customers	<input type="checkbox"/> Supplier management
<input type="checkbox"/> Employee Management (HR)	<input type="checkbox"/> Video surveillance-based security

**Required Information for the Record of processing activities (Art. 30.1 GDPR)**

**Data processing Controller. GDPR Art. 4.7**  
The figure of data controller RGPD, a legal figure defined in article 4.7 RGPD, which generally corresponds to a legal person, should not be confused with the allocation or distribution of responsibilities within the corresponding body/entity or the natural person who is the head of the responsible body. The CISO, CIO, CEO, human resources manager, general secretary, etc., are not controllers for the data processing operations of the entity to which they belong under RGPD.

Name and contact data of data processing controller and his/her representative (Art. 30.1.a)

Save changes and Open Risk management



<b>Key Points</b> .....	<b>2</b>
<b>What is a Data Protection Impact Assessment?</b> .....	<b>3</b>
<b>What are the benefits of conducting a DPIA?</b> .....	<b>3</b>
<b>How do I know if a DPIA should be conducted?</b> .....	<b>4</b>
<i>Evaluation or Scoring</i> .....	6
<i>Automated Decision Making with Significant Effects</i> .....	6
<i>Systematic Monitoring</i> .....	6
<i>Sensitive Personal Data</i> .....	7
<i>Data Processed on a Large Scale</i> .....	7
<i>Data Concerning Vulnerable Data Subjects</i> .....	8
<i>Innovation and Technology</i> .....	8
<i>International Transfers</i> .....	9
<i>Rights and Contractual Obligations</i> .....	9
<b>When is a DPIA not required?</b> .....	<b>10</b>
<b>Do DPIAs have to be renewed for existing processing operations?</b> .....	<b>10</b>
<b>When in a project lifecycle should a DPIA be conducted?</b> .....	<b>12</b>
<b>Who should be involved in conducting the DPIA?</b> .....	<b>12</b>
<b>What steps are involved in carrying out a DPIA?</b> .....	<b>14</b>
<b>Key stages of a successful DPIA</b> .....	<b>14</b>
1. <i>Identifying whether a DPIA is required</i> .....	15
2. <i>Describing the information flows</i> .....	15
3. <i>Identifying data protection and related risks</i> .....	16
<i>Potential Risks to Data Subjects</i> .....	18
4. <i>Identifying and evaluating data protection solutions</i> .....	19
5. <i>Signing off and recording the DPIA outcomes</i> .....	22
6. <i>Integrating the DPIA outcomes back into the project plan</i> .....	23
<b>Should the Data Protection Commission be consulted on completion of the DPIA?</b> .....	<b>23</b>
<b>Should the DPIA be published?</b> .....	<b>24</b>

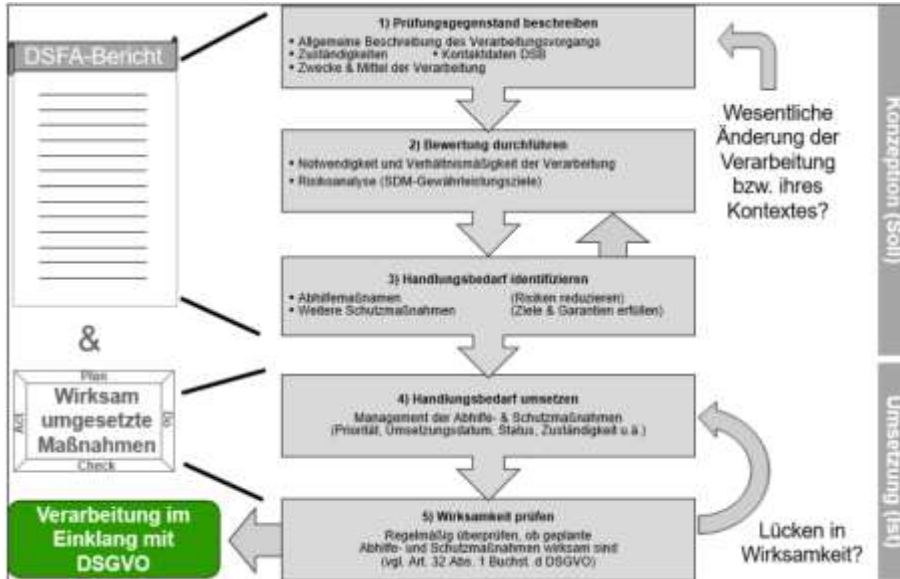
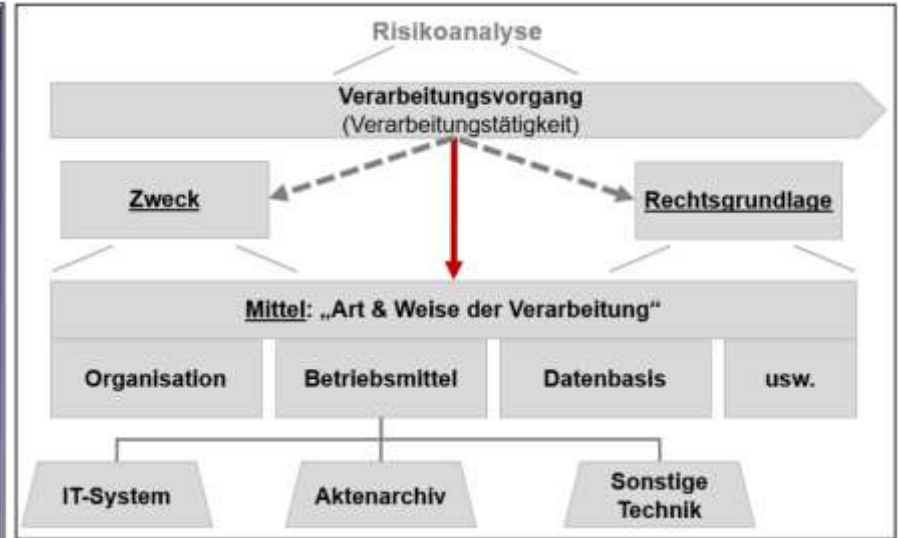
**agencia española protección datos** **Evalúa Riesgo RGPD**

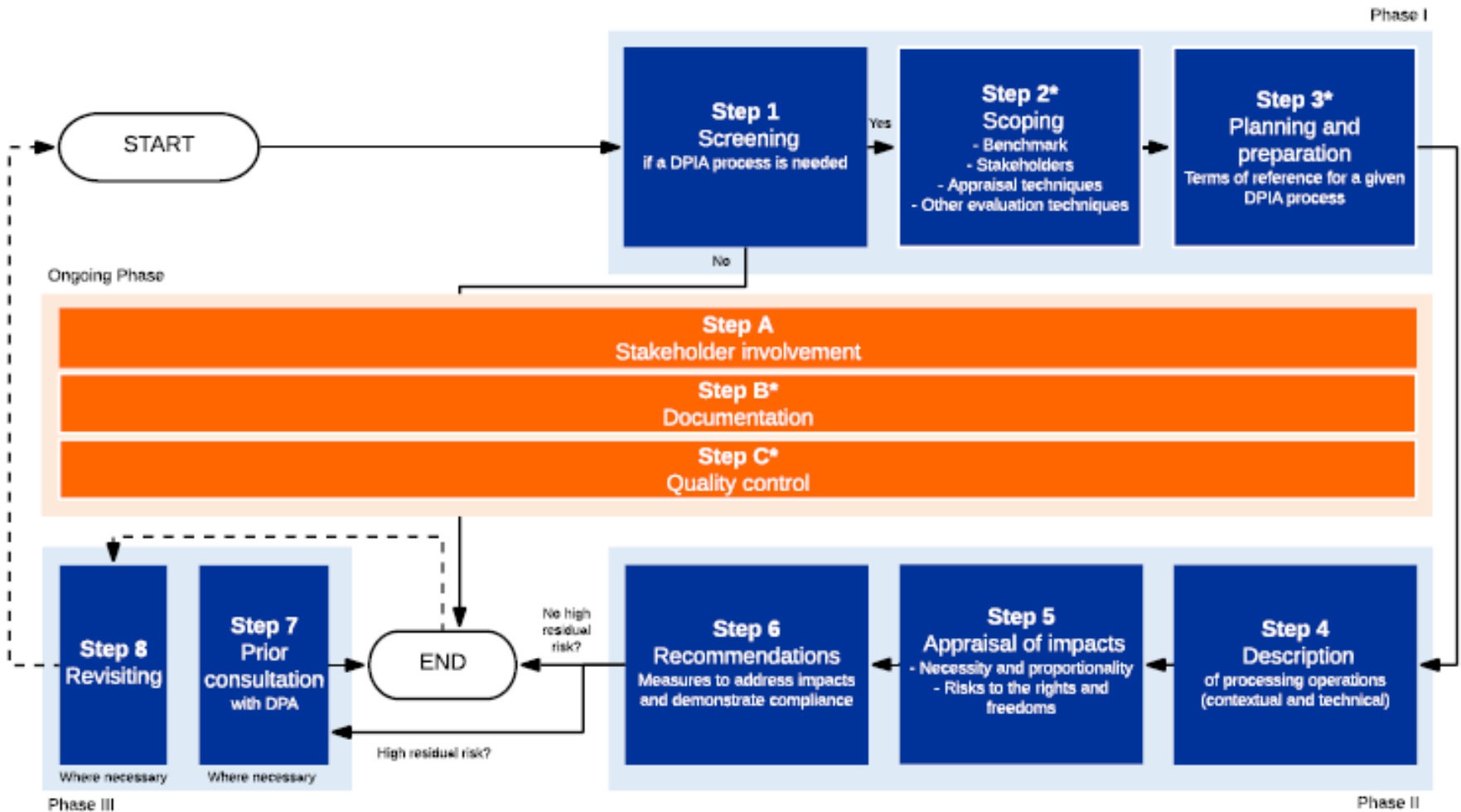
Finalidades Tipos Extensión Intereses Técnicos Recogida **Efectos** Responsables Comunicaciones Otros Seguridad Resultado ?

### Efectos colaterales del tratamiento

Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento. En este caso, no se ha evaluado por la AEPD el nivel de riesgo, sino solo el impacto que podría tener. El responsable tendrá que evaluar la probabilidad de que estas amenazas se materialicen en su tratamiento, por lo que se deja la columna "Probabilidad" vacía. Una vez completada, podrá determinar el nivel de riesgo empleando, por ejemplo, la matriz de riesgo "probabilidad e impacto" de la Guía.

Excede las expectativas del interesado	Probabilidad	Mitigación
<input type="checkbox"/> Exposición excesiva del interesado <input type="checkbox"/> Segmentación que excede expectativas razonables <input type="checkbox"/> Inferencia de intereses o de otras características en base a datos no evidentes y que derivan en un perfilado del sujeto <input type="checkbox"/> Otros	Improbable <span style="float: right;">Muy alta</span> <input type="range" value="0"/>	No Mitigado <span style="float: right;">Mitigado</span> <input type="range" value="0"/>
<b>Puede reversión no autorizada de la seudonimización</b> <input type="checkbox"/> Aplica	Improbable <span style="float: right;">Muy alta</span> <input type="range" value="0"/>	No Mitigado <span style="float: right;">Mitigado</span> <input type="range" value="0"/>
<b>Puede pérdida de control por el responsable de los datos procesados por el encargado del tratamiento</b> <input type="checkbox"/> Aplica	Improbable <span style="float: right;">Muy alta</span> <input type="range" value="0"/>	No Mitigado <span style="float: right;">Mitigado</span> <input type="range" value="0"/>
<b>Riesgo de reidentificación de usuarios</b> <input type="checkbox"/> Tratamientos de datos anonimizados <input type="checkbox"/> tratamientos de datos pseudonimizados <input type="checkbox"/> Riesgos de inferencia y vinculación <input type="checkbox"/> Otros	Improbable <span style="float: right;">Muy alta</span> <input type="range" value="0"/>	No Mitigado <span style="float: right;">Mitigado</span> <input type="range" value="0"/>
<b>Podría determinar la situación financiera</b> <input type="checkbox"/> Aplica	Improbable <span style="float: right;">Muy alta</span> <input type="range" value="0"/>	No Mitigado <span style="float: right;">Mitigado</span> <input type="range" value="0"/>
<b>Podría determinar la solvencia patrimonial</b> <input type="checkbox"/> Aplica	Improbable <span style="float: right;">Muy alta</span> <input type="range" value="0"/>	No Mitigado <span style="float: right;">Mitigado</span> <input type="range" value="0"/>
<b>Podría deducir información relacionada con categorías especiales de datos</b> <input type="checkbox"/> Aplica	Improbable <span style="float: right;">Muy alta</span> <input type="range" value="0"/>	No Mitigado <span style="float: right;">Mitigado</span> <input type="range" value="0"/>





## 168 Обзор Fieldfisher национальных «черных списков» DPIA

Country	Large-scale processing	New tech	Automated decision-making	Profiling and evaluation	Location data and tracking	Combining and matching data	Employee monitoring	Public surveillance	"Spectacle" processing	Children and vulnerable subjects	Bio-metric and genetic data	Data of a "highly personal nature"	Denial of service
Austria		✓	✓	✓	✗	✓		✓		✗	✗		
Belgium	✓	✓		✓	✓						✓	✓	✓
Bulgaria		✓			✓				✓	✓	✓		
Cyprus		✓		✓		✓	✓	✓			✓		
Czech Republic	✗	✗					✗	✗		✗	✗	✗	
Denmark		✗	✓	✓	✗					✗	✗		✗
France			✓	✓	✓		✓			✓	✓	✓	✓
Germany	✓		✓	✓	✓	✓	✓				✗		
Hungary	✓	✓	✓	✓	✓					✓	✓		✓
Ireland	✓		✓	✓	✓	✓	✓	✓		✓	✗		
Italy		✗	✓	✓	✓	✓	✓	✓		✓	✓	✓	
Luxembourg					✓	✓	✓	✓	✗		✗		
Netherlands	✓	✓		✓	✓		✓	✓			✓		
Norway		✗	✓	✓	✗						✗	✓	
Poland	✓	✓	✓	✓		✓	✓	✓			✓		✓
Slovakia		✗		✓		✓	✓	✓	✗		✗		✓
Slovenia	✓	✓	✓	✓		✓	✓	✓		✓	✓		✓
Spain	✗	✗	✗	✗	✗	✗	✗	✗		✗	✗	✗	✗
Sweden	✗	✗	✗	✗		✗	✓	✗		✗		✗	✗
United Kingdom		✗		✓	✗	✓			✗	✓	✗		✓

Fieldfisher подготовили материал, описывающий так называемые национальные «черные списки» Data Protection Impact Assessment (DPIA). Это списки, которые надзорные органы различных государств-членов ЕС обязаны публиковать в соответствии со статьей 35 (4) GDPR, и которые устанавливают, когда DPIA требуется для обработки операций, которые они контролируют. На январь 2020 года опубликовано 22 таких чёрных списка.





## Impact assessment shows privacy risks in Microsoft Office ProPlus Enterprise

*On behalf of the Dutch Ministry of Security and Justice, Privacy Company carried out a (DPIA) on Microsoft Office ProPlus (Office 2016 MSI and Office 365 CTR). At the request of the Ministry, we publish this blog about the findings. For questions about the research you can contact SLM Rijk (Strategic Vendor Management for Microsoft within the Ministry of Justice), accessible via the Press Office from the Ministry of Justice, +31 (0)70 370 73 45.*

The SLM Rijk conducts negotiations with Microsoft for approximately 300.000 digital work stations of the national government. The Enterprise version of the Office software is deployed by different governmental organisations, such as ministries, the judiciary, the police and the taxing authority.

The results of this Data Protection Impact Assessment (DPIA) are alarming. Microsoft collects and stores personal data about the behaviour of individual employees on a large scale, without any public documentation. The DPIA report (in English) as published by the Ministry is available [here](#).

Starting today, and with the help of Microsoft, SLM Rijk offers zero exhaust settings to admins of government organisations. During the writing of this DPIA, Microsoft has committed to take a number of other important measures to lower the data protection risks.

### Dutch Ministry of Security and Justice and Privacy Company

По поручению Министерства безопасности и юстиции Нидерландов компания Privacy Company осуществила Data Protection Impact Assessment в отношении продуктов Microsoft Office ProPlus (Office 2016 MSI и Office 365 CTR), используемых на 300,000 рабочих станций правительства Нидерландов. Результаты этой оценки воздействия на данные (DPIA) вызывают тревогу: Microsoft собирает и хранит данные о поведении отдельных работников в значительных масштабах, без какого-либо публичного документирования данной активности.

## 170 DPIA в отношении Microsoft Teams, OneDrive, SharePoint и Azure AD



Based on the ICO model, this results in the following matrix:<sup>195</sup>

<b>Severity of impact</b>	Serious harm	<b>Low risk</b> 1 <sup>196</sup> , 2, 3, 7	<b>High risk</b>	<b>High risk</b>
	Some impact	<b>Low risk</b> 6	<b>Medium risk</b>	<b>High risk</b>
	Minimal impact	<b>Low risk</b>	<b>Low risk</b>	<b>Low risk</b> 4, 5
		Remote	Reasonable possibility	More likely than not
		<b>Likelihood of harm (occurrence)</b>		

<https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad>

<https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad/Public+DPIA+Teams+OneDrive+SharePoint+and+Azure+AD+16+Feb+2022.pdf>

# 171 DPIA в отношении Google Workspace (G Suite) Enterprise

Based on the ICO model, this results in the following matrix:

<b>Severity of impact</b>	Serious harm	Low risk 11, 12, 13	High risk 8	High risk 1, 2, 3, 4, 5, 6, 7,9, 10
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		<b>Likelihood of harm (occurrence)</b>		

## Scope Data Protection Impact Assessment G Suite Enterprise

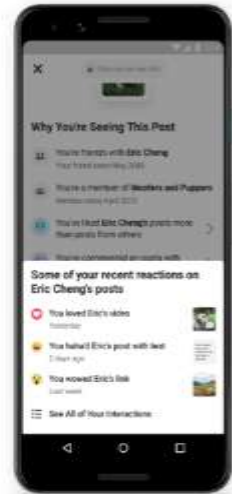
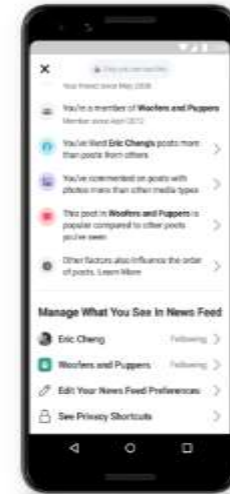
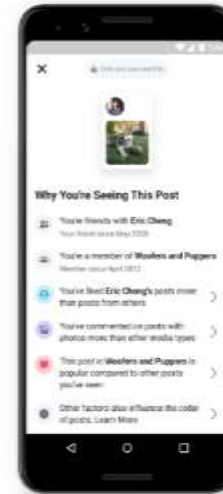


<https://www.privacycompany.eu/blogpost-en/privacy-assessment-google-workspace-g-suite-enterprise-dutch-government-consults-dutch-data-protection-authority-on-high-privacy-risks>

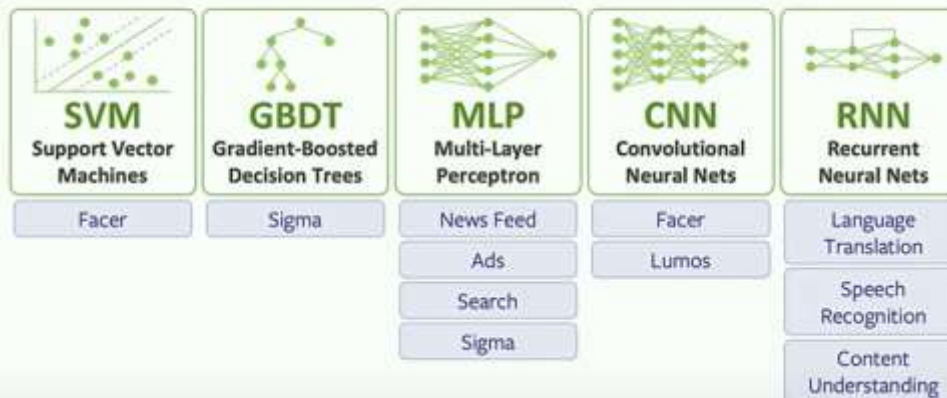
<https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2021/02/12/google-workspace-dpia-for-dutch-dpa/Google+Workspace+DPIA+for+Dutch+DPA+v18+Feb+2021.pdf>

## DPIA в отношении официальных аккаунтов госорганов Нидерландов в соцсети Facebook

Severity of impact	Serious harm	Low risk 8	High risk 2, 5, 6, 7	High risk 1, 3, 4
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
	Likelihood of harm (occurrence)			



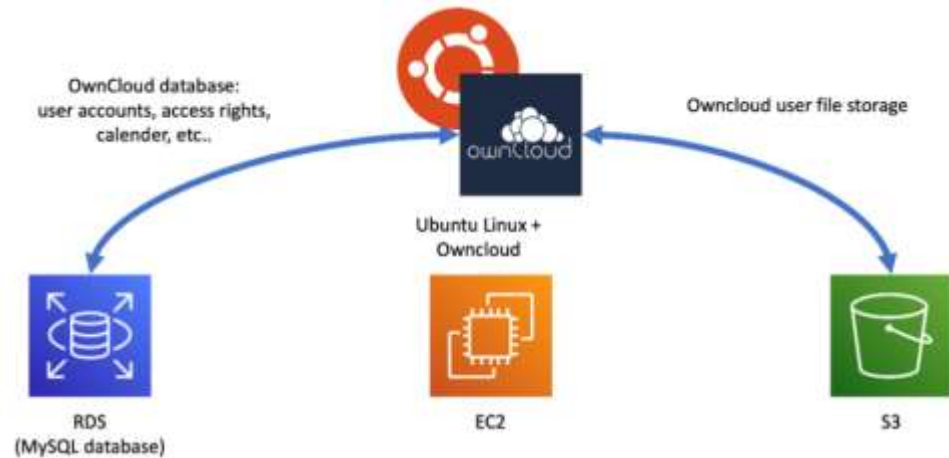
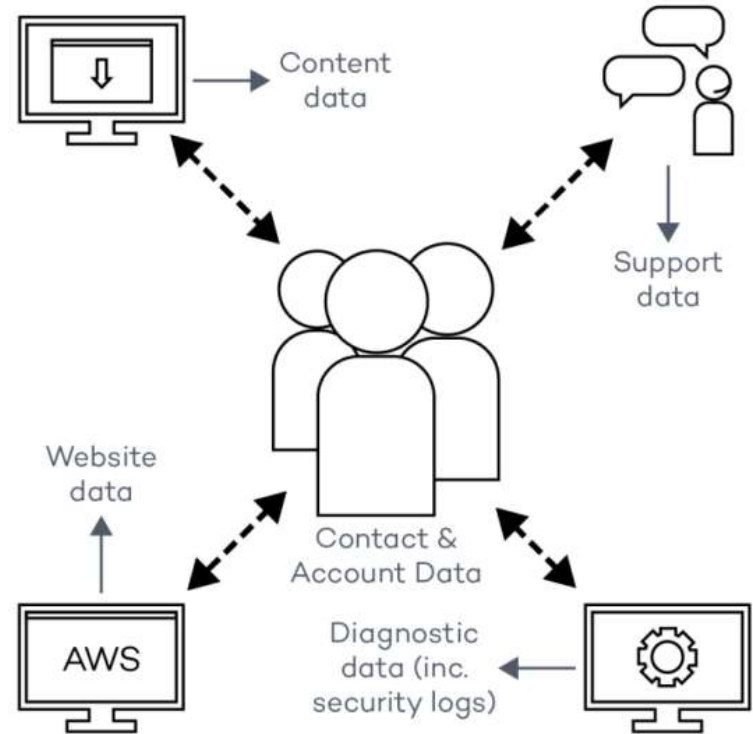
### Major Services and Algorithms



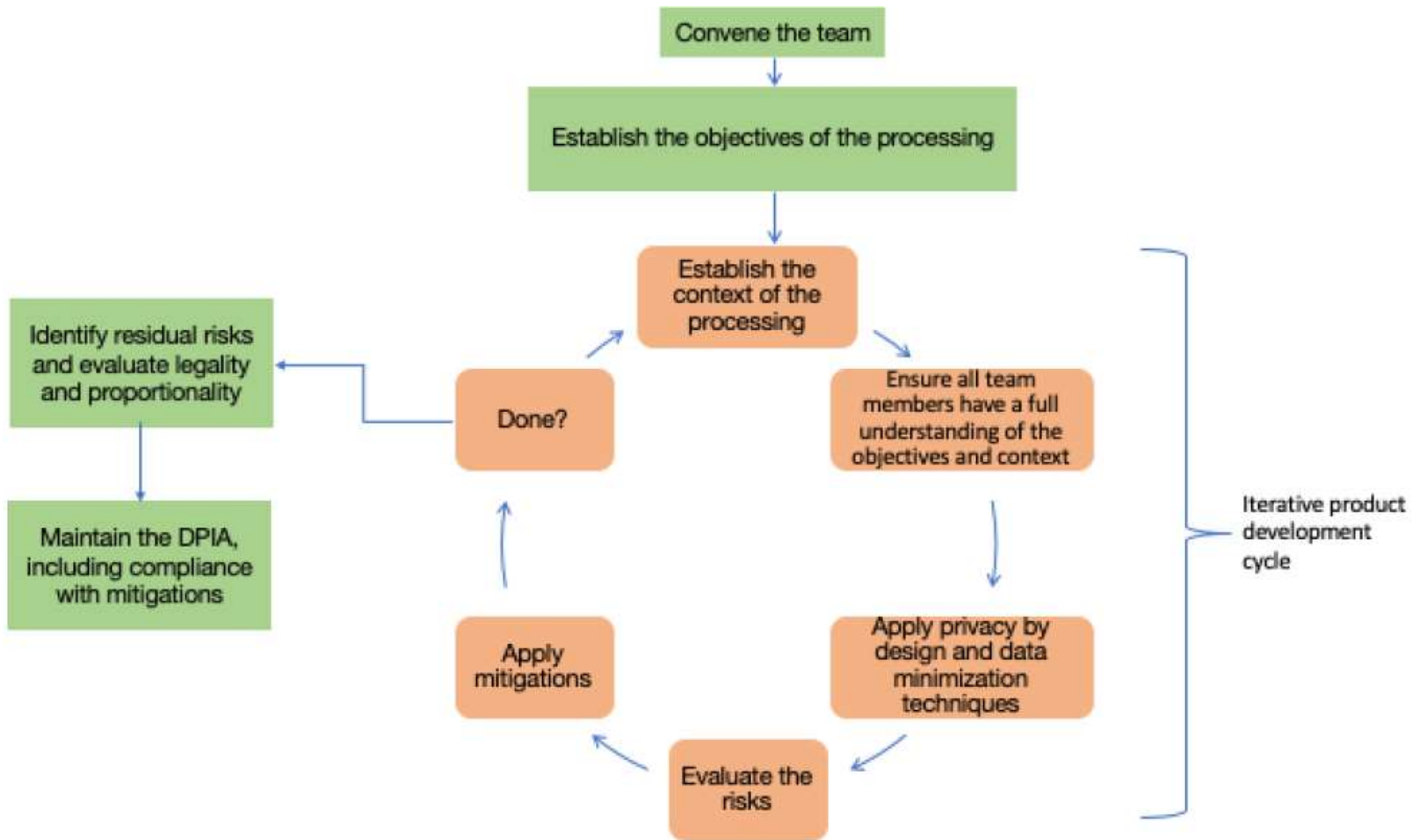
# 173 DPIA в отношении Amazon Web Services

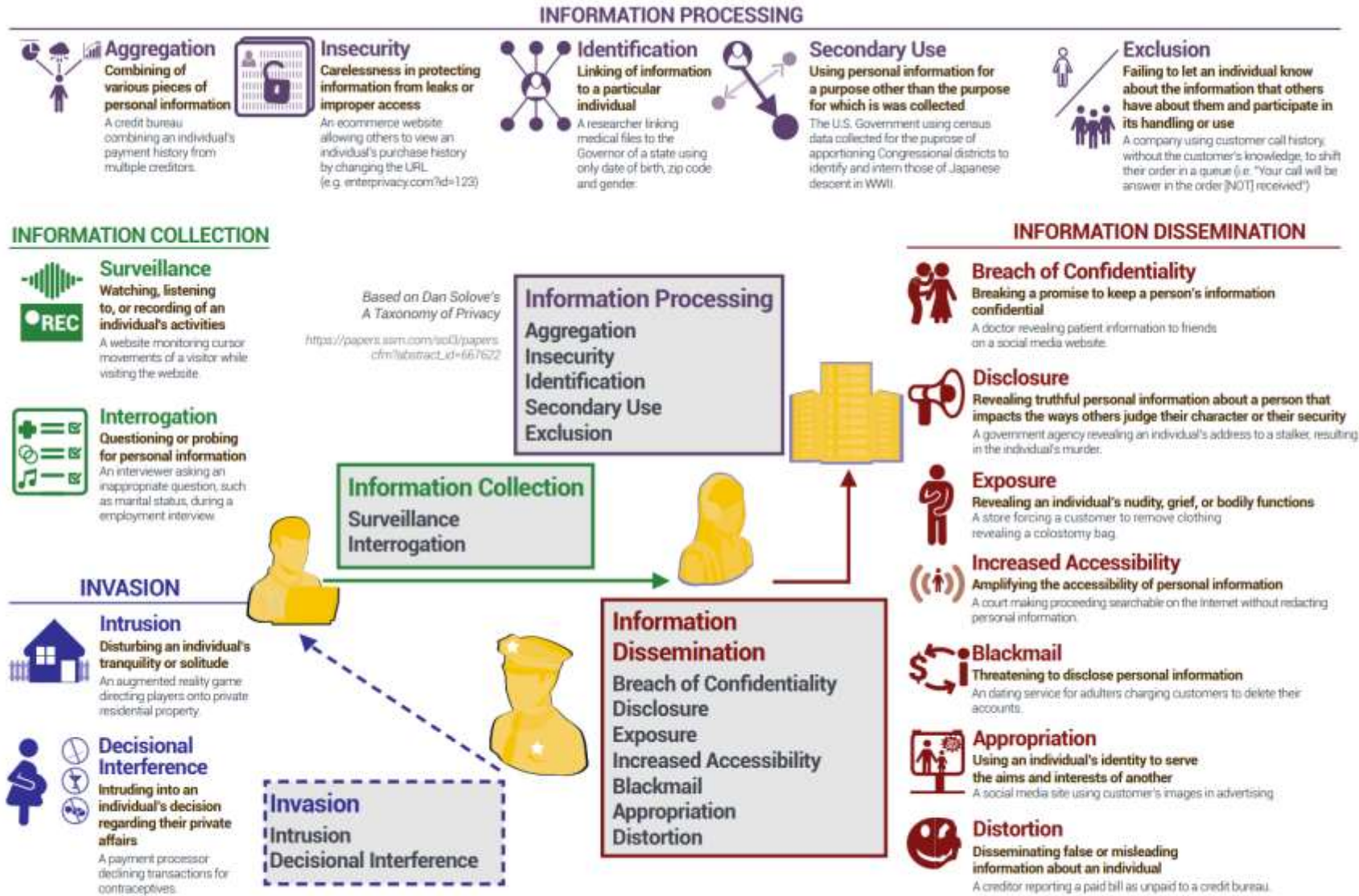
Table 3: Risk assessment

<b>Severity of impact</b>	<b>Serious harm</b>	<b>Low risk</b> 1, 6, 7, 8b	<b>High risk</b>	<b>High risk</b>
	Some impact	<b>Low risk</b>	<b>Medium risk</b>	<b>High risk</b>
	Minimal impact	<b>Low risk</b> 2, 8a	<b>Low risk</b>	<b>Low risk</b> 3, 4, 5, 9
		Remote	Reasonable possibility	More likely than not
		<b>Likelihood of harm (occurrence)</b>		



## 174 Рекомендации IAB Europe по осуществлению DPIA





## Typology of Privacy Harms

Danielle Keats Citron and Daniel J. Solove





## PRIVACY HARMS

DANIELLE KEATS CITRON\* &amp; DANIEL J. SOLOVE\*\*

## ABSTRACT

*The requirement of harm has significantly impeded the enforcement of privacy law. In most tort and contract cases, plaintiffs must establish that they have suffered harm. Even when legislation does not require it, courts have taken it upon themselves to add a harm element. Harm is also a requirement to establish standing in federal court. In Spokeo, Inc. v. Robins and TransUnion LLC v. Ramirez, the Supreme Court ruled that courts can override congressional judgment about cognizable harm and dismiss privacy claims.*

*Case law is an inconsistent, incoherent jumble with no guiding principles. Countless privacy violations are not remedied or addressed on the grounds that there has been no cognizable harm.*

*Courts struggle with privacy harms because they often involve future uses of personal data that vary widely. When privacy violations result in negative consequences, the effects are often small—frustration, aggravation, anxiety, inconvenience—and dispersed among a large number of people. When these minor harms are suffered at a vast scale, they produce significant harm to individuals, groups, and society. But these harms do not fit well with existing cramped judicial understandings of harm.*

*This Article makes two central contributions. The first is the construction of a typology for courts to understand harm so that privacy violations can be tackled and remedied in a meaningful way. Privacy harms consist of various different types that have been recognized by courts in inconsistent ways. Our*

\* Jefferson Scholars Foundation Schenck Distinguished Professor in Law, Caddell and Chapman Professor of Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; 2019 MacArthur Fellow.

\*\* John Marshall Harlan Research Professor of Law, George Washington University Law School.

## CONTENTS

INTRODUCTION .....	796
I. COGNIZABLE HARMS: THE LEGAL RECOGNITION OF PRIVACY HARMS .....	799
A. <i>Standing</i> .....	800
B. <i>Harm in Causes of Action</i> .....	807
1. Contract Law .....	807
2. Tort Law .....	808
3. Statutory Causes of Action.....	810
C. <i>Harm in Regulatory Enforcement Actions</i> .....	813
II. THE CHALLENGES OF PRIVACY HARMS .....	816
A. <i>Aggregation of Small Harms</i> .....	816
B. <i>Risk: Unknowable and Future Harms</i> .....	817
C. <i>Individual vs. Societal Harms</i> .....	818
III. REALIGNING PRIVACY ENFORCEMENT AND REMEDIES .....	819
A. <i>The Goals of Enforcement</i> .....	820
B. <i>Aligning Remedies with Goals</i> .....	820
1. The Problem of Misalignment.....	820
2. The Value of Private Enforcement.....	821
3. An Approach for Realignment .....	822
IV. THE IMPORTANCE OF PROPERLY RECOGNIZING PRIVACY HARMS .....	826
A. <i>Properly Identifying the Interests at Stake</i> .....	826
B. <i>The Expressive Value of Recognizing Harm</i> .....	828
C. <i>Legislative and Regulatory Agenda</i> .....	829
V. A TYPOLOGY OF PRIVACY HARMS .....	830
A. <i>Physical Harms</i> .....	831
B. <i>Economic Harms</i> .....	834
C. <i>Reputational Harms</i> .....	837
D. <i>Psychological Harms</i> .....	841
1. Emotional Distress .....	841
2. Disturbance.....	844
E. <i>Autonomy Harms</i> .....	845
1. Coercion .....	846
2. Manipulation .....	846
3. Failure to Inform .....	848
4. Thwarted Expectations.....	849
5. Lack of Control .....	853
6. Chilling Effects.....	854
F. <i>Discrimination Harms</i> .....	855
G. <i>Relationship Harms</i> .....	859
CONCLUSION.....	861

## 178 Рекомендации RPPA по осуществлению DPIA

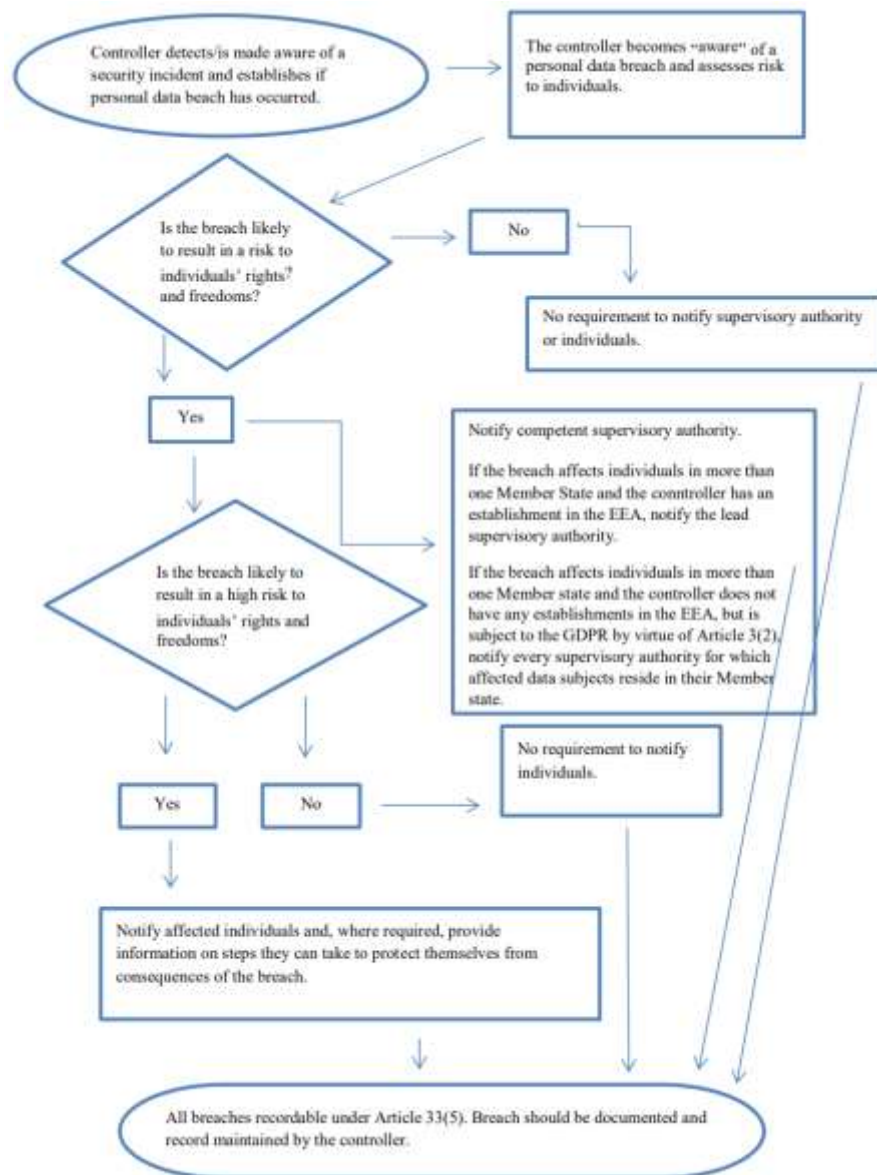
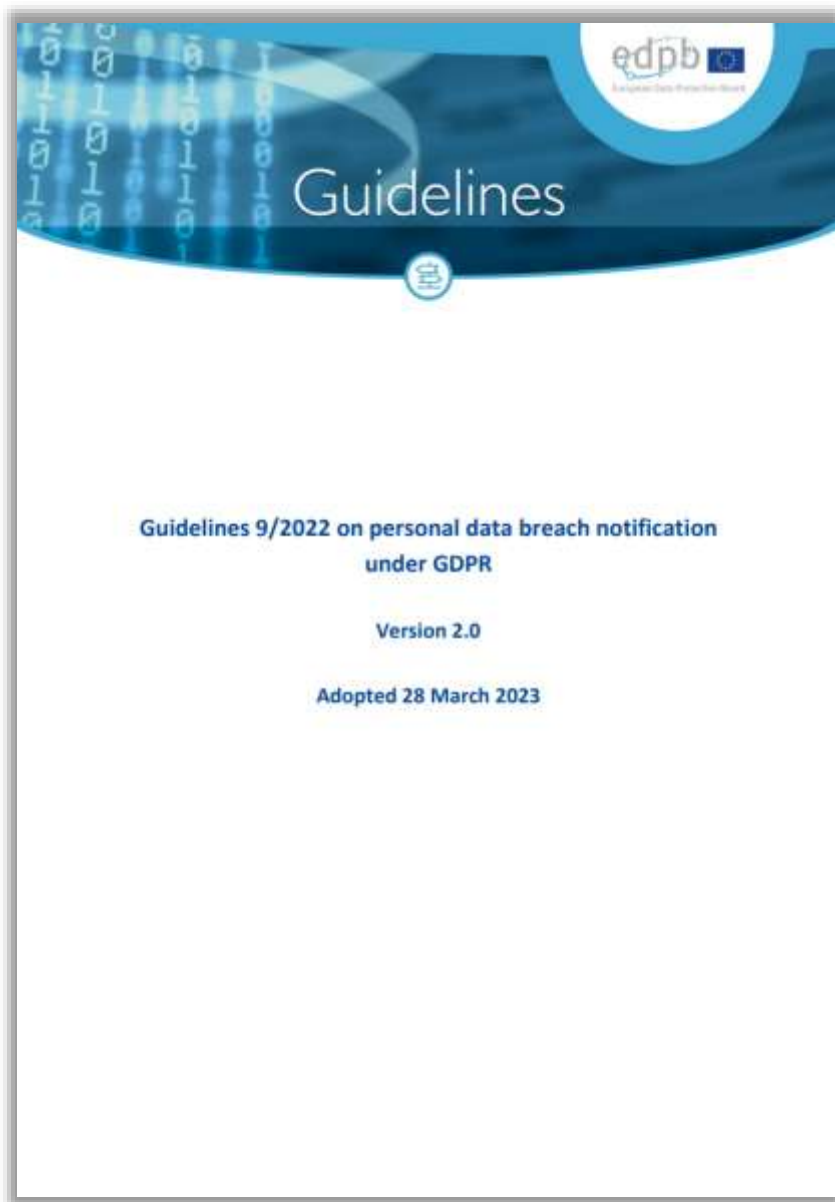
Нарушение статей	Зрелость	Риск	Зрелость	Риск	Зрелость	Риск
Законность обработки (6)	1	49.58	1	49.58	4	5.06
Принципы обработки (5)	1	26.46	3	6.79	4	4.29
Права субъектов (12,15-22)	1	6.42	2	4.82	1	6.42
Информирование субъекта (13,14)	1	33.76	1	33.76	3	6.92
Безопасность (25,32)	1	189.38	3	24.22	4	5.92
Взаимодействие с регуляторами (33,77)	1	5.99	2	4.86	3	4.86

[Участники Russian Privacy Professionals Association](#) могут ознакомиться с [материалами семинара в виде презентации и шаблона DPIA](#) (для получения доступа к материалам необходимо зайти в свою учетную запись на сайте).

Type	Risks to the company	Risks to the rights and freedoms of natural persons
<b>Focus on</b>	Consequences for organizations	Privacy impacts on individuals
<b>Initiator</b>	Chief Privacy Officer (CPO)	Data Protection Officer (DPO)
<b>Approach</b>	Enterprise Risk Management	<ul style="list-style-type: none"> <li>Data Protection Impact Assessment (DPIA)</li> <li>Transfer risk assessments (TRA)</li> </ul>
<b>Purpose</b>	To identify and prepare for hazards with a company's finances, operations, and objectives. To choose a privacy compliance strategy.	To choose and implement appropriate technical and organisational measures.
<b>Related to</b>	<ul style="list-style-type: none"> <li>Enterprise GRC</li> <li>Privacy Strategy</li> <li>Privacy Program</li> </ul>	<ul style="list-style-type: none"> <li>Privacy by Design</li> <li>Privacy Program</li> <li>Information Security Program</li> </ul>
<b>Consequence / Impact</b> (ISO 27557)	<ul style="list-style-type: none"> <li>Noncompliance costs (regulatory fines, litigation costs, remediation costs)</li> <li>Direct business costs (revenue or performance loss from customer abandonment or avoidance)</li> <li>Damage to reputation (brand damage, loss of customer trust)</li> <li>Harm to internal organizational culture (impact on capability of organization /unit to achieve vision/mission, impact on productivity / employee morale stemming from conflicts with internal cultural values or ethics)</li> </ul>	<ul style="list-style-type: none"> <li>Dignity loss (includes embarrassment and emotional distress)</li> <li>Discrimination</li> <li>Economic loss (can include direct financial losses as the result of identity theft or the failure to receive fair value in a transaction)</li> <li>Loss of self-determination (Loss of autonomy / Loss of liberty / Physical harm)</li> <li>Loss of trust</li> </ul>
<b>Special conditions for High risks</b>	No restrictions, Top management makes the decision	The controller shall consult the supervisory authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
<b>Methodology</b>	ISO 31000, COSO ERM ISO 27005 (for data breach risks)	Supervisory authorities' guidelines (EDPB/WP29, ICO, DPC, CNIL, AEPD, APDCAT, PDPC...)

# Data Breach Management





## WHAT IS A PERSONAL DATA BREACH?

A **personal data breach** is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Not every information security incident is a personal data breach, but every personal data breach is an information security incident.

Personal data breaches may occur due to:

- human errors, when information is emailed to the wrong person;
- loss or theft of devices containing non-encrypted personal data;
- weak authentication methods which allow unauthorised access to databases.

## WHAT TO DO IN CASE OF A PERSONAL DATA BREACH?

- Identify the personal data breach incident.
- Notify the breach to your Data Protection Officer (DPO), this is an **obligation** under EU data protection law.
- Handle the data breach **immediately** to mitigate any immediate risks for individuals' personal data.
- Document the breach, this is the principle of **accountability**.
- Assess the impact of the personal data breach on individuals' rights and freedoms.
- If you are a **processor**, you must immediately notify the controller of your organisation or EU institution.
- As an EU institution, office, body or agency (EUI), you are obliged to notify the European Data Protection Supervisor without undue delay and, where feasible, no later than 72 hours after the breach.
- Communicate the personal data breach to the impacted individuals if necessary.
- Review your procedures and update your measures.

## WHAT ARE THE TYPES OF BREACHES THAT MAY OCCUR?

- **Confidentiality breach:** an entity or person accessing personal data that they are not entitled to.
- **Availability breach:** losing access to and control of their personal data, or deleting misappropriated personal data.
- **Integrity breach:** whenever there is an inappropriate modification of personal data.

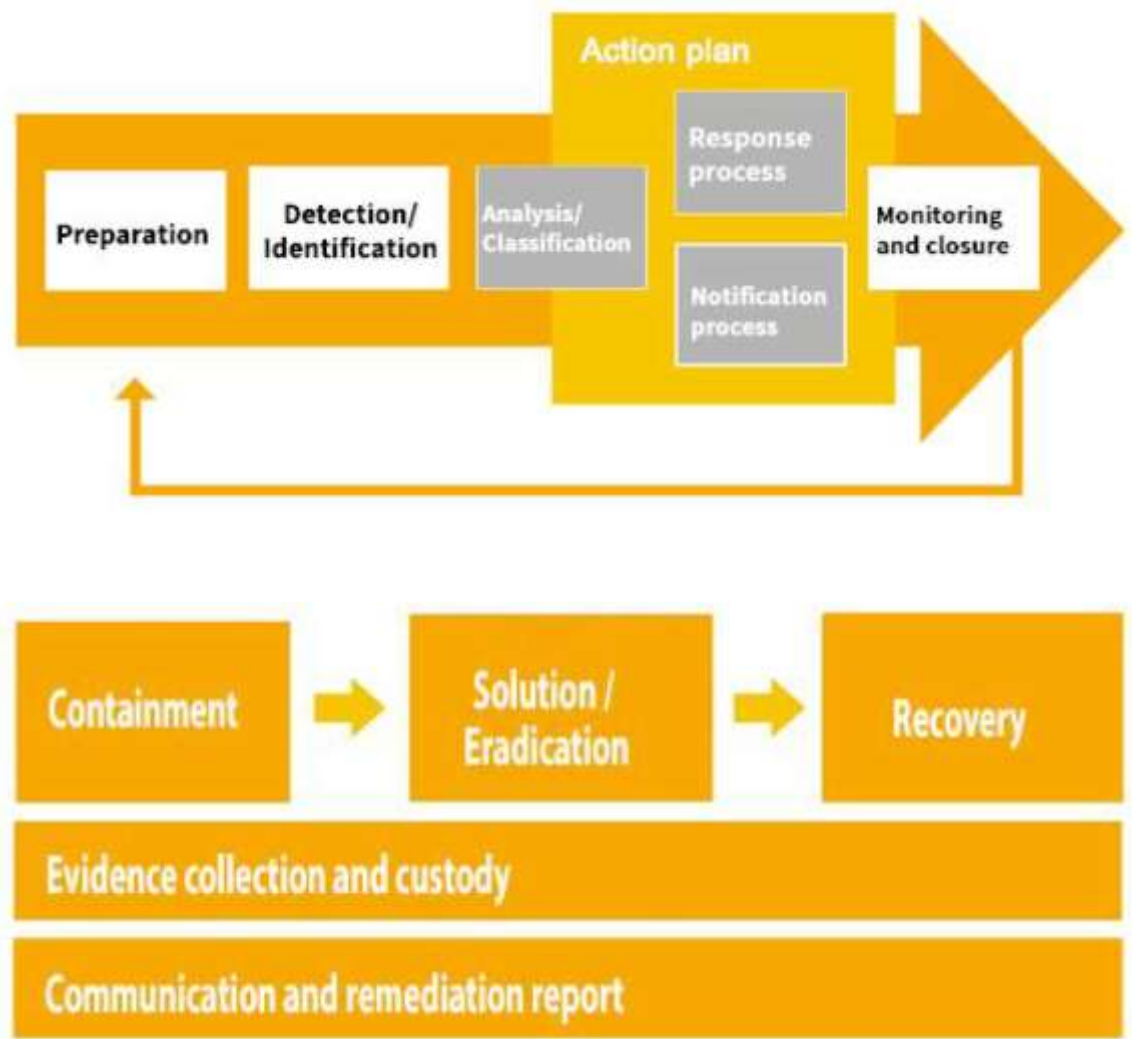
## WHO IS INVOLVED WHEN A PERSONAL DATA BREACH OCCURS?

- Top management (accountable)
- Business owner
- DPO
- IT department (if needed)
- Processors (if needed)
- Communication team (if needed)

## WHAT DOES A DPO DO?

A DPO:

- provides advice on the assessment of the impact to the data subjects and on the necessity of Personal Data Breach notifications, when requested;
- recommends mitigation measures;
- is the contact person for individuals;
- is the contact person for the EDPS;
- communicates with security officers on Information Security Risk Management and data breach policy;
- prepares and delivers awareness programmes for employees.



## Консультативный инструмент по уведомлению о нарушении безопасности данных от испанского AEPD



agencia española protección datos

Instrucciones Obligación Brecha Responsabilidad Competencia Riesgo Confidencialidad

Obligación de notificar brechas

Respecto a la brecha de datos personales, usted es:

- Una persona que se ha visto afectada por una brecha de datos personales ocurrida en una entidad que trata afiliado, administrado, estudiante, empleado, etc.
- Una persona conocedora de una brecha de datos personales, pero no ha visto afectados sus datos.
- Quien representa o pertenece a una entidad que trata datos personales y desea asesoramiento sobre la notificación a la Agencia Española de Protección de Datos.

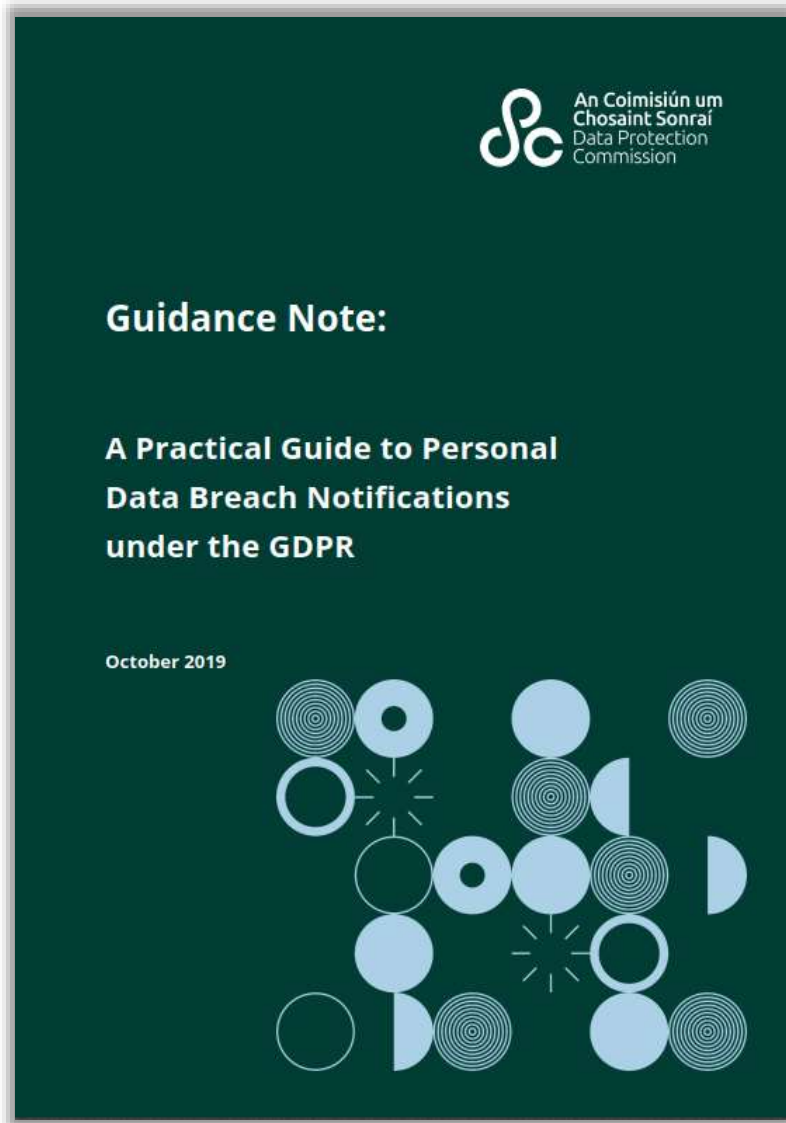
Испанский орган по защите данных ("AEPD") 25.10.2022 объявил о запуске консультативного инструмента "Asesora Brecha", который призван помочь контролерам данных решить, следует ли им уведомлять надзорный орган о нарушении персональных данных. Данный инструмент является бесплатным и может быть использован DPO, менеджерами по обработке данных или консультантами для получения адекватной информации, с помощью которой они могут консультировать контролеров данных.

Кроме того, данный инструмент дает рекомендации по следующим вопросам:

- кто должен уведомить надзорный орган;
- какие ситуации соответствуют нарушению безопасности данных, а какие нет;
- кто является компетентным надзорным органом;
- необходимо ли уведомлять о нарушении безопасности данных в зависимости от степени риска.



## Практическое руководство ирландского DPC по уведомлениям о нарушениях безопасности данных



Ирландский надзорный орган DPC (Data Protection Commission) провел анализ полученных уведомлений об утечках персональных данных (Data Breach Notification) из различных государственной и частных сфер, таких как банковское дело и финансы, страхование, телекоммуникации, здравоохранение, правоохранительные органы, и опубликовал в октябре 2019 года Руководство, посвящённое разбору типичных ошибок при осуществлении уведомлений об утечке данных:

- несвоевременное уведомление;
- сложность в оценке рейтингов риска;
- неспособность сообщить об утечке субъектам данных, где это применимо;
- повторные уведомления об утечках;
- предоставление неполной и неточной информации.

## Практическое руководство датского Datatilsynet по предотвращению нарушений безопасности данных

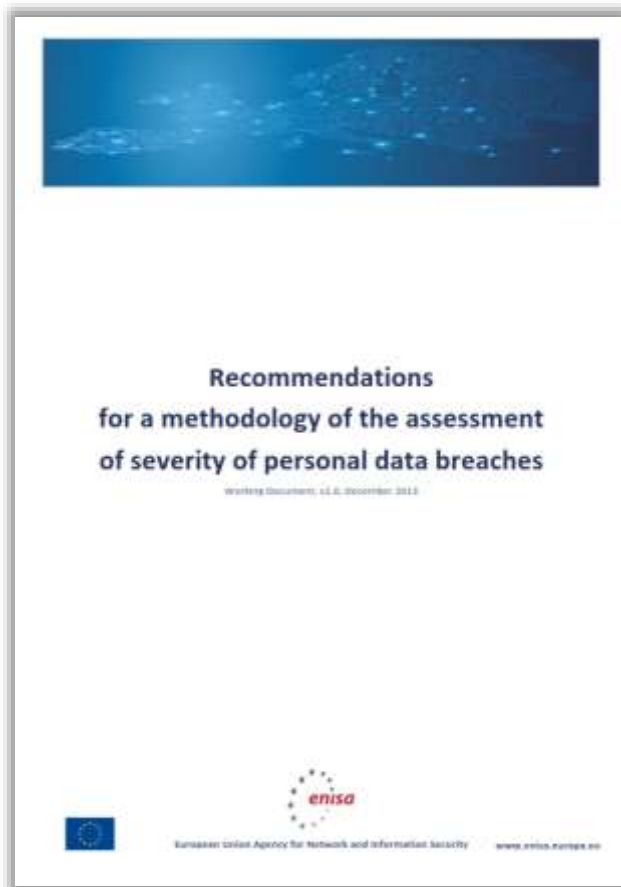


Датский орган по защите данных (Datatilsynet) 08.01.2023 опубликовал руководство по предотвращению нарушений безопасности данных. В документе рассказывается о типичных случаях нарушения безопасности данных и даются рекомендации по мерам безопасности, которые можно предпринять для снижения риска нарушения безопасности.

Руководство выделяет следующие распространенные типы нарушений безопасности данных:

- отправка данных неверному получателю из-за того, что неверный адресат был объединен в исходящем электронном сообщении;
- использование функции автозаполнения для отправки писем неверным адресатам;
- раскрытие защищенных адресов после изменения ИТ-системы;
- неправильное обращение с данными во время обработки;
- неспособность удалить данные с помощью цифровых инструментов;
- потеря/кража портативных устройств с незашифрованными данными;
- неограниченный доступ к данным на сетевых дисках;
- несанкционированный доступ к данным из-за плохого дизайна, ошибок в разработке ПО и недостаточного тестирования;
- раскрытие данных, хранящихся в шаблонах и формах;
- вредоносное ПО (ransomware), приводящее к потере и неправомерному использованию данных.

## Рекомендации от ENISA по выработке методологии оценки тяжести нарушений безопасности персональных данных



### Definition of severity level

As introduced in the Section 2.2, the overall severity (SE) is calculated by the following formula:

$$SE = DPC \times EI + CB$$

The final score shows the level of severity of a certain breach, taking into account the impact to the individuals<sup>8</sup>.

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE < 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

## 188 Статистика количества Data Breach в 2018-2021 годах от DLA Piper (1)



■ From 25 May 2018 to 27 January 2022

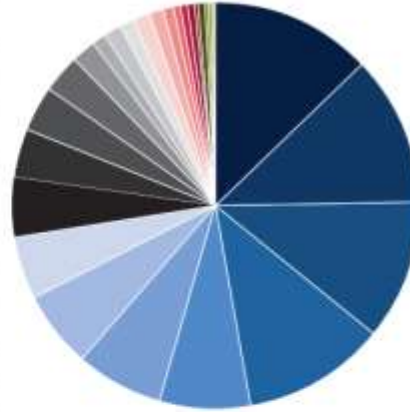


■ From 28 January 2021 to 27 January 2022

■ From 28 January 2020 to 27 January 2021

## 189 Статистика количества Data Breach в 2018-2021 годах от DLA Piper (2)

Per capita country ranking of breach notifications*	Number of breach notifications per 100,000 population between 28 January 2021 and 27 January 2022 (last 12 month period)	Change compared to last year's ranking
Netherlands	150.71	+1
Liechtenstein	136.02	+6
Denmark	130.60	-2
Ireland	130.19	-1
Finland	85.59	No change
Germany*	79.42	+3
Slovenia	71.70	-3
Luxembourg	57.76	-1
Sweden	54.83	+1
Norway	44.12	+1
Iceland	43.91	-5
Poland	33.75	+1
Malta	22.23	-1
Estonia	14.97	+1
Belgium	14.37	+2
UK*	14.14	-2
Lithuania	13.97	+3
Hungary	13.53	No change
Austria	9.60	-3
Cyprus	7.98	-1
France	6.88	+3
Slovakia	4.97	Information not previously publically available
Latvia	4.89	-2
Spain	4.28	-2
Italy	2.86	+1
Croatia	2.48	-1
Czech Republic	2.25	-4
Greece	1.45	No change

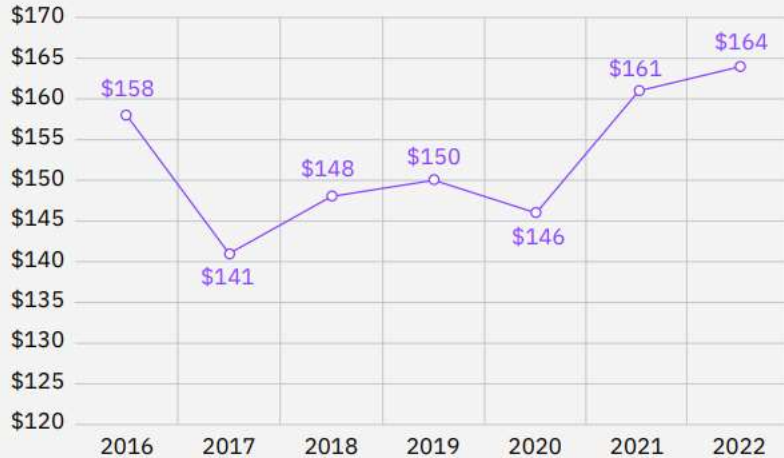


# 190 Отчет IBM от 2022 года о стоимости утечек данных

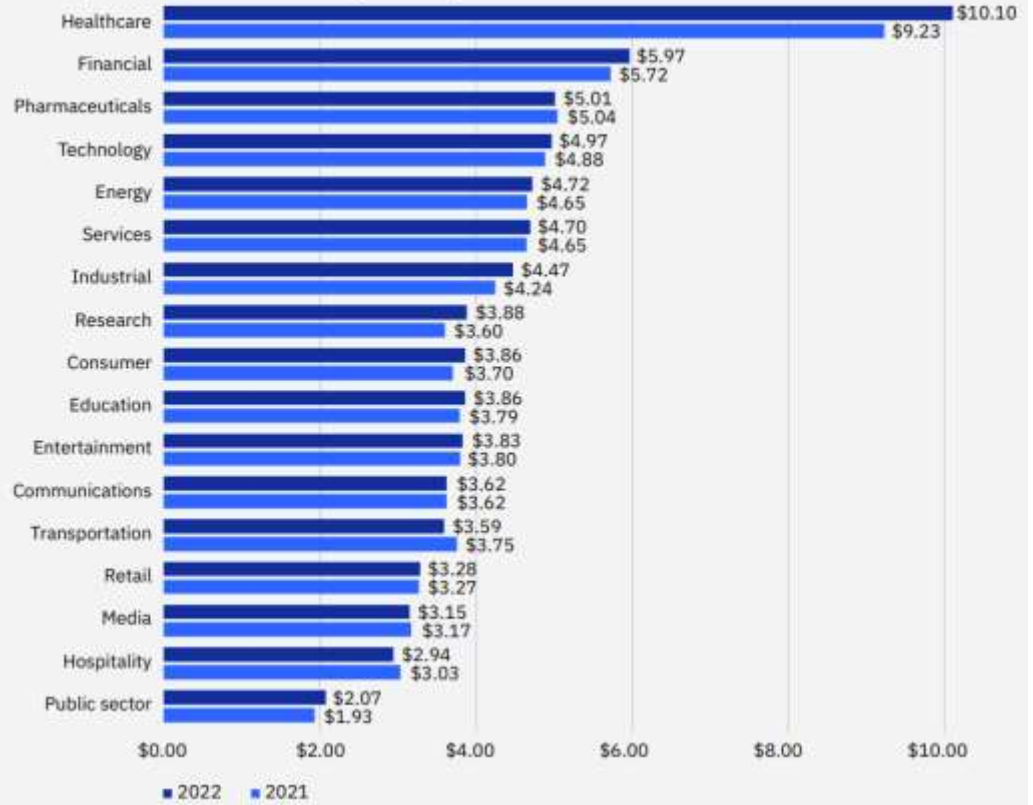
Average total cost of a data breach

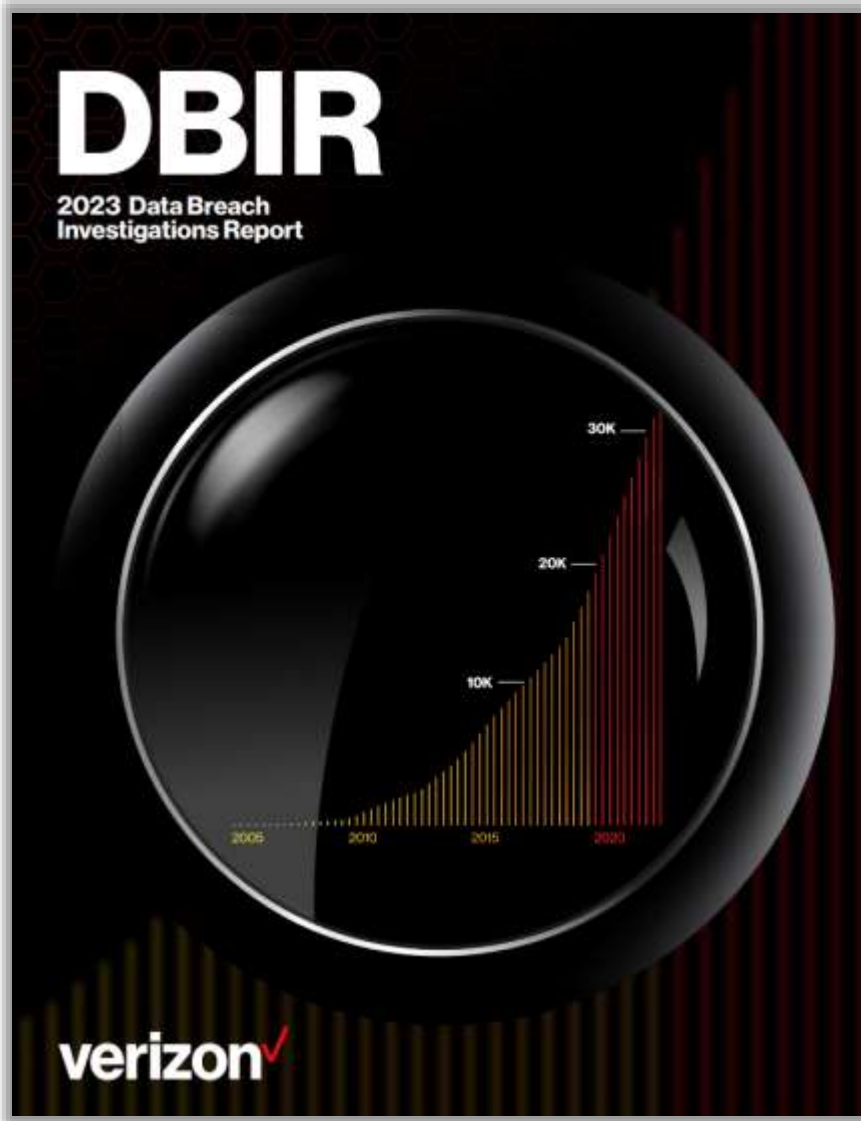


Average per record cost of a data breach



Average cost of a data breach by industry





0% 20% 40% 60% 80% 100%

83% of breaches involved External actors (n=5,177)



74% of breaches involved a human element (n=4,482)



49% of breaches involved credentials (n=4,396)

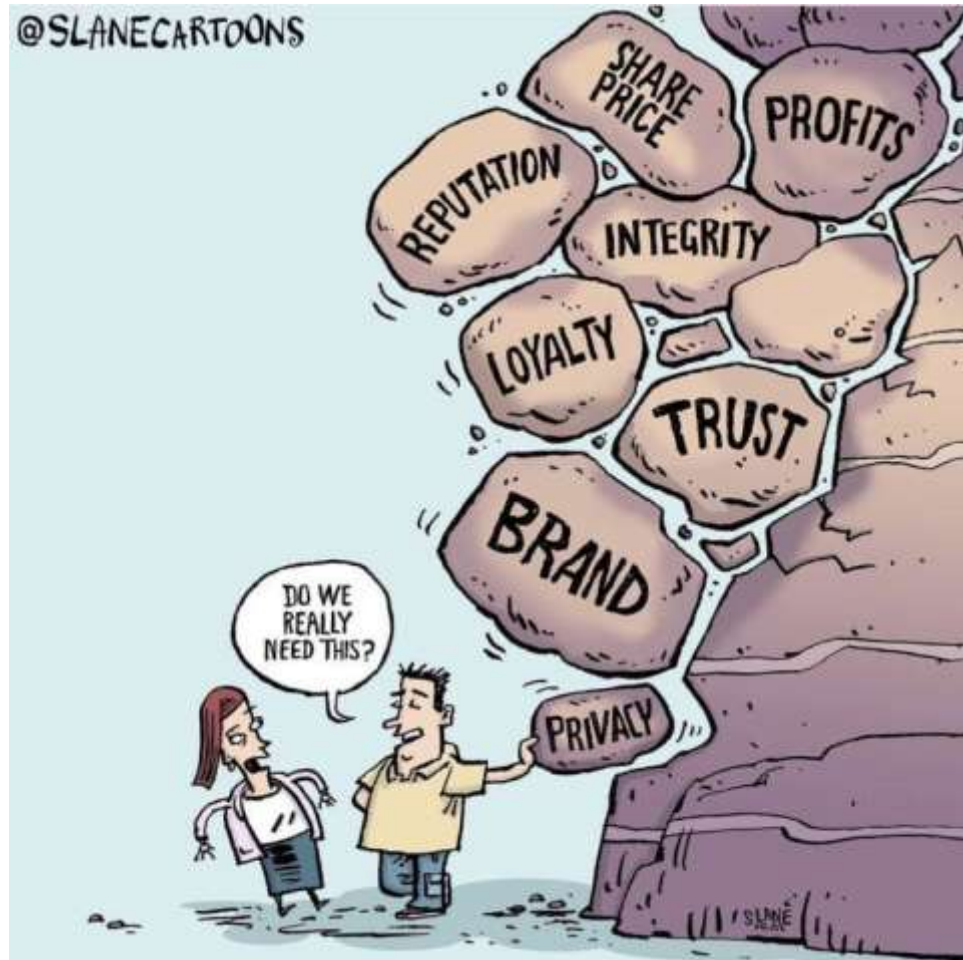


24% of breaches involved Ransomware (n=4,354)



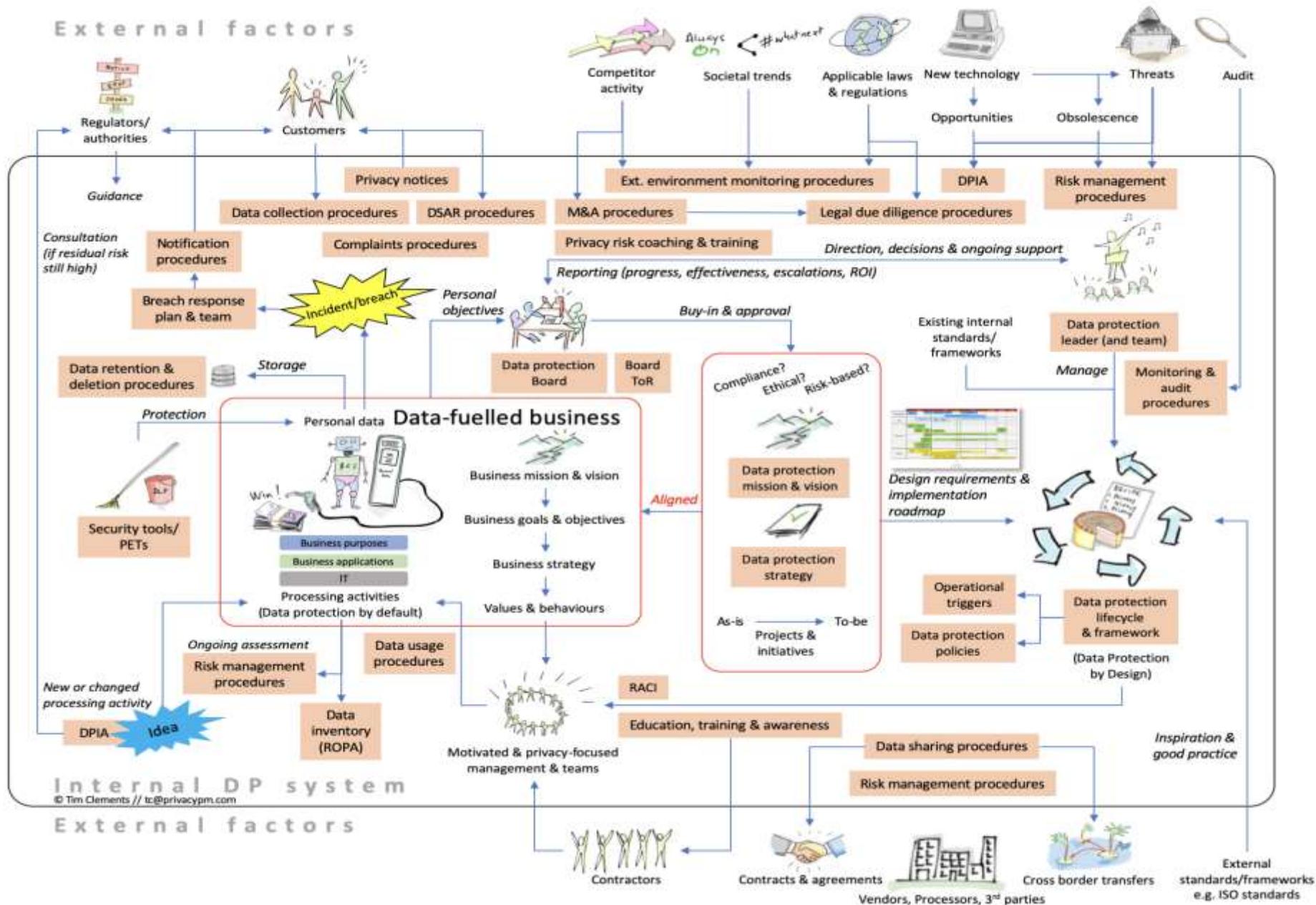
0% 20% 40% 60% 80% 100%

# Data Protection Officer





# Представление системы управления обработкой и защитой персональных данных в организации



# DPO как медиатор в процессах комплаенса по персональным данным



**Организационные функции**

1

- › Создание и поддержание реестра процессов обработки персональных данных
- › Изучение и анализ процессов обработки персональных данных
- › Оценка рисков, связанных с процессами обработки персональных данных, проведение оценки воздействия на защиту данных (DPIA)

**Контроль соблюдения функций**

- › Управление нарушениями безопасности обработки ПДн
- › Проведение расследований по нарушениям процедур надлежащей обработки ПДн

3

**Консультации и сотрудничество с надзорными органами (Data Protection Authorities, DPA)**

4

**Консультативные функции**

- › Поддержка и продвижение концепций Privacy by Design and by Default
- › Консультирование и мониторинг соблюдения локальных актов контролера и соглашений с третьими лицами в сфере приватности
- › Поддержка участия контролера в кодексах надлежащего поведения и системах сертификации

2

**5 Обработка запросов субъектов данных****Информирование и повышение осведомленности**

6

- › Информирование и повышение осведомленности субъектов данных и иных лиц (сотрудников, партнеров, поставщиков, клиентов, общественность, СМИ и т. д.)
- › Планирование и анализ деятельности DPO

Обработка органом власти, субъектом властных полномочий

- Public body

Регулярное систематическое наблюдение в больших объёмах

- Мониторинг через «умные» устройства
- Трекинг местонахождения
- Видеомониторинг
- Программы лояльности
- Поведенческая реклама
- Создание профилей и скоринг для оценки рисков

Обработка больших объёмов специальных категорий данных

- Медицинские данные
- Данные о сексуальной ориентации
- Генетические данные
- Данные о политических и религиозных взглядах
- Данные об этническом происхождении
- Данные о членстве в профсоюзе
- Биометрические данные для идентификации

Обработка больших объёмов данных о судимости и правонарушениях

- Данные о правонарушениях
- Данные об уголовных приговорах
- Данные о нарушении правил безопасности

### Rec.97

DPO, вне зависимости от того, являются ли они работниками контролера, должны быть в состоянии независимо исполнять свои обязанности и выполнять свои задачи.

### Art.38(1)

Контролер или процессор должны гарантировать, что DPO принимает своевременное и надлежащее участие в решении всех вопросов, связанных с защитой персональных данных

### Art.38(3)

Контролер или процессор должны гарантировать, что DPO не получает иных указаний относительно выполнения указанных задач.

DPO не должен быть отстранен или оштрафован контролером или процессором за выполнение своих задач.

### Art.38(6)

DPO может выполнять иные задачи и обязанности. Контролер или процессор должны гарантировать, что любые такие задачи и обязанности не влекут за собой конфликт интересов.

- DPO может являться работником контролера или процессора, или он может выполнять задачи на основе договора об оказании услуг. Соответственно, у него есть материальная и иная личная **заинтересованность** в продолжении выполнения своих функций.
- DPO является уважаемым и **сертифицированным** профессионалом, обладающим экспертными знаниями законодательства и практики в области защиты данных, а также дорожающим своей **репутацией**.



## 199 Модели конфликта интересов: DPO-босс



Роль DPO выполняет один из руководителей организации, который сталкивается с конкурирующими интересами при принятии решений. Как DPO он должен защищать права и законные интересы субъектов персональных данных. Как топ-менеджер (уровня финансового или ИТ-директора) он оценивает «стоимость» своих решений для организации, и на практике интересы компании оказываются для него приоритетны.

## 200 Модели конфликта интересов: DPO-сам-себе-контролер



У меня не бывает приступов лени,  
иногда бывают приступы активности...

Роль DPO выполняет работник, принимающий решения в важной области ИТ-инфраструктуры (ИТ-менеджер, системный администратор, ответственный за эксплуатацию информационных систем, в которой обрабатываются персональные данные, и др.). DPO вынужден сам контролировать свою работу. Это создает предпосылки для внутреннего конфликта интересов: в большинстве ситуаций для такого работника приоритетны текущие задачи и риски в его основной области.



## 201 Модели конфликта интересов: DPO-мастер-на-все-руки



Роль DPO поручена работнику, который выполняет рекомендации, написанные им же. В качестве DPO работник выявляет риски в сфере защиты данных и разрабатывает рекомендации по снижению этих рисков. В роли внутреннего консультанта он разрабатывает локальные документы (согласия, политики, положения и даже техническую документацию) и контролирует их внедрение в организации. В результате конфликта интересов работник упрощает себе задачу — разрабатывает план действий с минимальными затратами времени и сил.

## De jure

- Детальное и исчерпывающее описание роли и функций DPO в локальных нормативных актах
- Определение и закрепление в договоре между DPO и его нанимателем взаимных прав и обязанностей
- Наделение DPO правом инициировать обсуждение критически важных вопросов с руководством организации-нанимателя

## De facto

- Признание ведущей роли экспертизы DPO в вопросах, касающихся персональных данных
- Предоставление DPO всех необходимых для выполнения функций сведений или возможностей для их получения
- Готовность руководства организации-нанимателя добросовестно рассмотреть вопросы, вынесенные DPO на обсуждение

Создание и укрепление доверия между DPO и его нанимателем



## Court of Justice of the European Union

*Judgment in Case C-453/21  
X-FAB Dresden GmbH & Co. KG v FC*

Суд Европейского Союза ("CJEU") 09.02.2023 вынес предварительное решение по делу C-453/21 X-FAB Dresden GmbH & Co. KG v FC по запросу Федерального суда по трудовым спорам Германии ("Суд по трудовым спорам") в отношении ст. 38(3) и 38(6) GDPR касательно увольнения сотрудника компании X-FAB с должности DPO.

CJEU постановил, что второе предложение ст.38(3) GDPR не препятствует принятию национального законодательства, предусматривающего, что контроллер или процессор может уволить внутреннего DPO только при наличии уважительной причины, даже если увольнение не связано с выполнением задач этого DPO, в той мере, в какой такое законодательство не подрывает достижение целей GDPR.

CJEU высказал мнение, что ст.38(6) GDPR должна быть истолкована как означающая, что "конфликт интересов" может существовать, когда на DPO возложены другие задачи или обязанности, в результате которых он будет определять цели и методы обработки персональных данных со стороны контроллера или его процессора. Существование конфликта интересов в таких случаях должен определять национальный суд в каждом конкретном случае, оценивая все соответствующие обстоятельства, включая организационную структуру контроллера или процессора, и, в свете всех применимых правил, любую политику контроллера или процессора.

# Data Protection Officer Requirements by Country

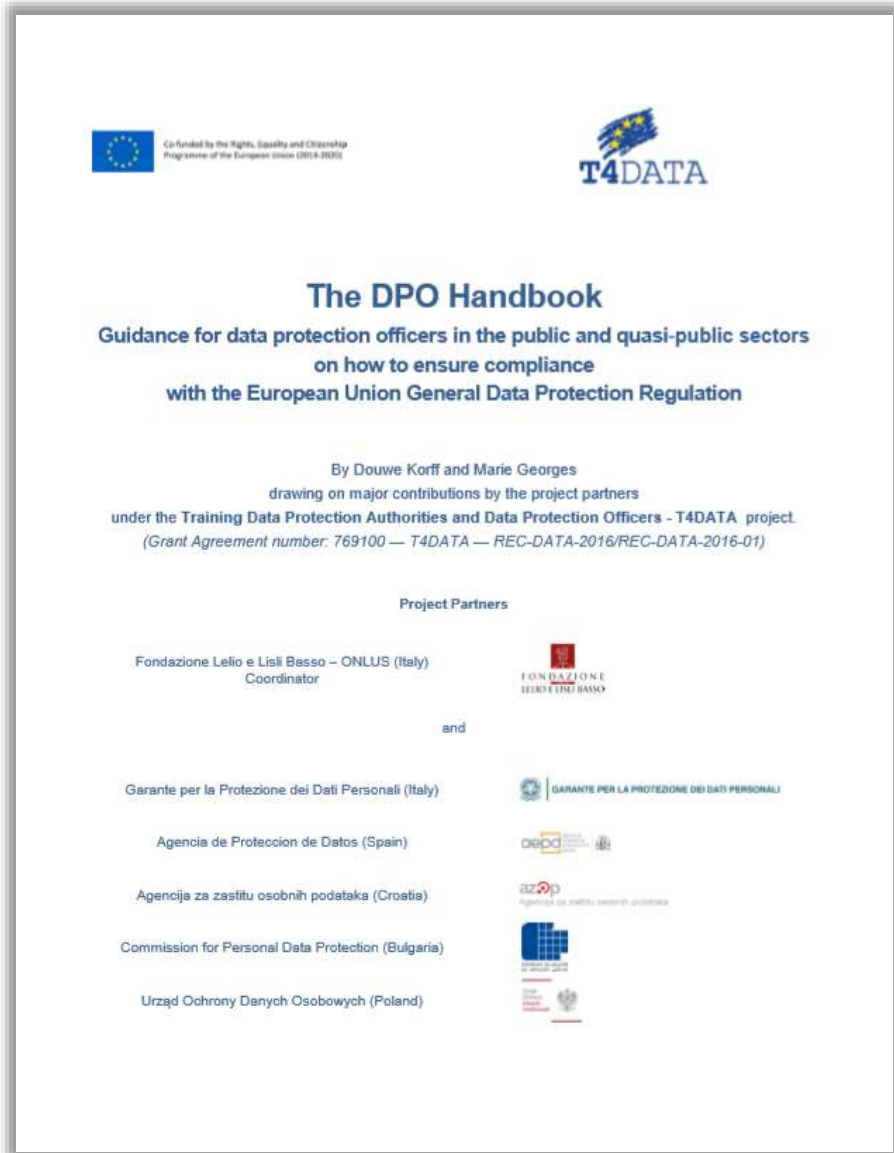


Increasingly, privacy and data protection laws around the world require organizations to designate a data protection officer to translate legal protections into practical reality. This chart catalogues those requirements but does not include the many additional instances in which a DPO is recommended but not required. If you are aware of additional material that should be included here, please email the Westin Research Center at [research@iapp.org](mailto:research@iapp.org).

	Legal instrument	Terminology	Scope	Tasks	Structure	Training/expertise	Registration/notification
Australia	Privacy (Australian Government Agencies — Governance) APP Code 2017	<ul style="list-style-type: none"> <li>Designate a privacy officer.</li> </ul>	<ul style="list-style-type: none"> <li>Government agencies.</li> </ul>	<ul style="list-style-type: none"> <li>Provide the agency advice on privacy matters.</li> <li>Handle internal and external privacy enquiries, complaints and requests for access to and correction of personal information.</li> <li>Maintain a record of the agency's PI holdings.</li> <li>Assist with the preparation of privacy impact assessments and maintain the agency's register of PIAs.</li> <li>Measure and document the agency's performance against the privacy management plan at least annually.</li> </ul>	<ul style="list-style-type: none"> <li>An agency may have one or more privacy officers.</li> <li>The privacy officer may serve as the required privacy champion, or the two positions may be separate.</li> </ul>	<ul style="list-style-type: none"> <li>The Office of the Australian Information Commissioner's "Privacy Officer Toolkit" describes useful skills and expertise and offers resources for privacy officers.</li> </ul>	<ul style="list-style-type: none"> <li>Provide the OAIC contact information for the privacy officer in writing.</li> </ul>
Bermuda	Personal Information Protection Act Part 2, Section 5	<ul style="list-style-type: none"> <li>Designate a representative ("privacy officer").</li> </ul>	<ul style="list-style-type: none"> <li>All organizations.</li> </ul>	<ul style="list-style-type: none"> <li>Take responsibility for compliance with the act.</li> <li>Communicate with the commissioner.</li> </ul>			<ul style="list-style-type: none"> <li>Publish name of privacy officer in privacy notice.</li> </ul>



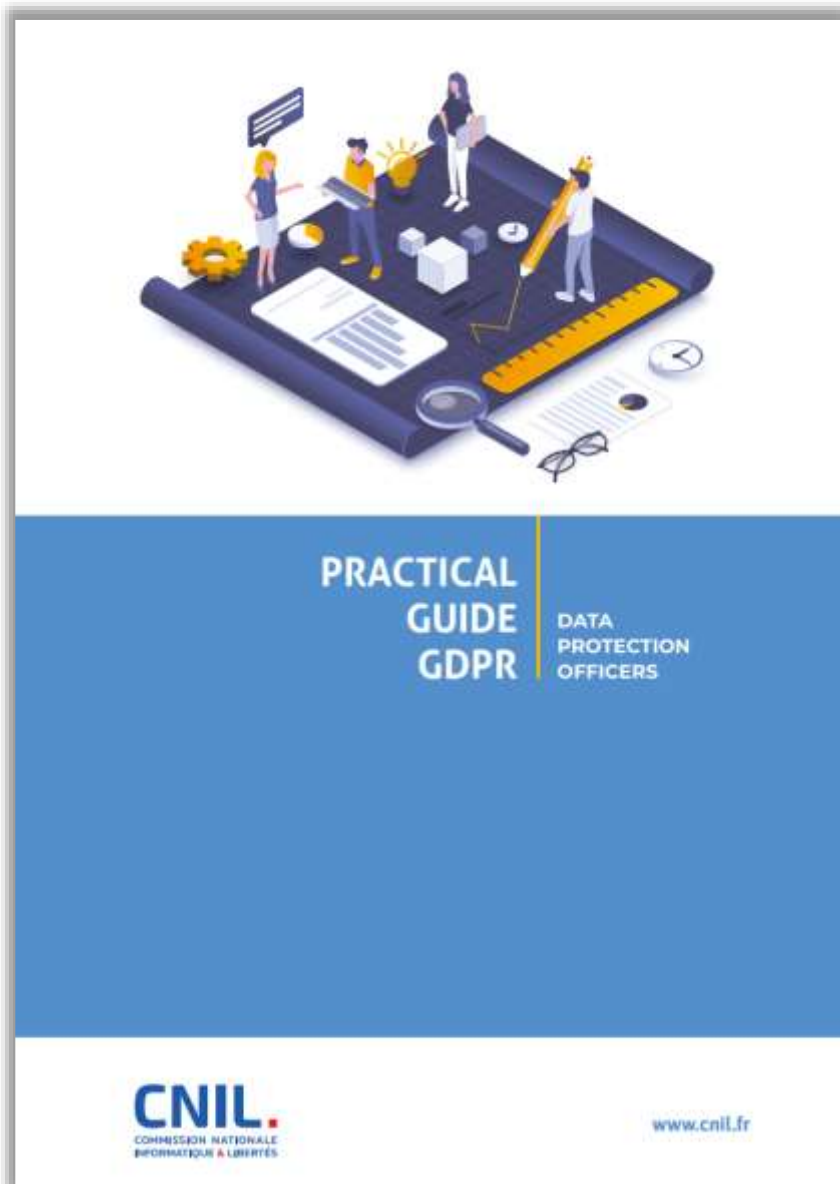
- 1 INTRODUCTION .....
- 2 DESIGNATION OF A DPO .....
- 2.1 MANDATORY DESIGNATION .....
- 2.1.1 'Public authority or body' .....
- 2.1.2 'Core activities' .....
- 2.1.3 'Large scale' .....
- 2.1.4 'Regular and systematic monitoring' .....
- 2.1.5 Special categories of data and data relating to criminal convictions and offences.....
- 2.2. DPO OF THE PROCESSOR .....
- 2.3. DESIGNATION OF A SINGLE DPO FOR SEVERAL ORGANISATIONS.....
- 2.4. ACCESSIBILITY AND LOCALISATION OF THE DPO.....
- 2.5. EXPERTISE AND SKILLS OF THE DPO .....
- 2.6. PUBLICATION AND COMMUNICATION OF THE DPO'S CONTACT DETAILS .....
- 3 POSITION OF THE DPO .....
- 3.1. INVOLVEMENT OF THE DPO IN ALL ISSUES RELATING TO THE PROTECTION OF PERSONAL DATA .....
- 3.2. NECESSARY RESOURCES .....
- 3.3. INSTRUCTIONS AND 'PERFORMING THEIR DUTIES AND TASKS IN AN INDEPENDENT MANNER' .....
- 3.4. DISMISSAL OR PENALTY FOR PERFORMING DPO TASKS .....
- 3.5. CONFLICT OF INTERESTS.....
- 4 TASKS OF THE DPO .....
- 4.1. MONITORING COMPLIANCE WITH THE GDPR .....
- 4.2. ROLE OF THE DPO IN A DATA PROTECTION IMPACT ASSESSMENT .....
- 4.3. COOPERATING WITH THE SUPERVISORY AUTHORITY AND ACTING AS A CONTACT POINT .....
- 4.4. RISK-BASED APPROACH .....
- 4.5. ROLE OF THE DPO IN RECORD-KEEPING .....
- 5 ANNEX - DPO GUIDELINES: WHAT YOU NEED TO KNOW .....
- DESIGNATION OF THE DPO.....
- 1 WHICH ORGANISATIONS MUST APPOINT A DPO? .....
- 2 WHAT DOES 'CORE ACTIVITIES' MEAN? .....
- 3 WHAT DOES 'LARGE SCALE' MEAN? .....
- 4 WHAT DOES 'REGULAR AND SYSTEMATIC MONITORING' MEAN? .....
- 5 CAN ORGANISATIONS APPOINT A DPO JOINTLY? IF SO, UNDER WHAT CONDITIONS? .....
- 6 WHERE SHOULD THE DPO BE LOCATED? .....
- 7 IS IT POSSIBLE TO APPOINT AN EXTERNAL DPO?.....
- 8 WHAT ARE THE PROFESSIONAL QUALITIES THAT THE DPO SHOULD HAVE? .....
- POSITION OF THE DPO.....
- 9 WHAT RESOURCES SHOULD BE PROVIDED TO THE DPO BY THE CONTROLLER OR THE PROCESSOR? .....
- 10 WHAT ARE THE SAFEGUARDS TO ENABLE THE DPO TO PERFORM HER/HIS TASKS IN AN INDEPENDENT MANNER? WHAT DOES 'CONFLICT OF INTERESTS' MEAN? .....
- TASKS OF THE DPO .....
- 11 WHAT DOES 'MONITORING COMPLIANCE' MEAN? .....
- 12 IS THE DPO PERSONALLY RESPONSIBLE FOR NON-COMPLIANCE WITH DATA PROTECTION REQUIREMENTS? .....
- 13 WHAT IS THE ROLE OF THE DPO WITH RESPECT TO DATA PROTECTION IMPACT ASSESSMENTS AND RECORDS OF PROCESSING ACTIVITIES? .....



## The DPO Handbook

На сайте итальянского регулятора (Garante per la protezione dei dati personali) опубликовано «Руководство для DPO» от T4DATA (за авторством двух специалистов - Douwe Korff и Marie Georges) на английском языке, которое касается деятельности DPO в государственном и квазигосударственном секторах.

Руководство описывает роль и функции DPO, цитируются документы и позиции европейских национальных DPA, WP29, CEDPO и других относительно каждого аспекта деятельности DPO. Также даются пояснения относительно существующих систем сертификации DPO, определяются требования к знаниям, квалификации, опыту, личным качествам DPO.



<b>2</b>	<b>FOREWORD</b>
<b>3</b>	<b>WHAT ARE THE CNIL'S MISSIONS?</b>
<b>4</b>	<b>THE ROLE OF THE DPO</b>
4	Advising and supporting the organisation
6	Monitoring the effectiveness of the rules
6	Being the organisation's point of contact on GDPR matters
7	Ensuring the documentation of data processing
<b>10</b>	<b>DESIGNATING THE DPO</b>
12	Factsheet 1: In which cases should a DPO be appointed?
14	Factsheet 2: Who can be designated DPO?
20	Factsheet 3: Internal or external DPO? How can the function be shared?
24	Factsheet 4: How to appoint a DPO?
<b>28</b>	<b>PERFORMING THE FUNCTION OF DPO</b>
28	Factsheet 5: what resources should be allocated to the DPO?
32	Factsheet 6: What is the status of the DPO?
36	Factsheet 7: What to do in the event of departure, leave or replacement of the DPO?
<b>38</b>	<b>HOW DOES THE CNIL SUPPORT DPOS?</b>
38	Tools for training
38	Tools for finding an answer
39	Compliance tools
<b>40</b>	<b>FAQ</b>
40	I am looking for a DPO for my organisation, what should I do?
40	What does the designation of a DPO bring if my organisation already has a legal department responsible for data protection?
41	Where should the DPO be located?
41	What language should the DPO speak?
42	Is the title of "data protection officer - DPO" reserved for persons designated with the CNIL?
42	How can a DPO be trained?
<b>43</b>	<b>APPENDICES</b>
43	Appendix No. 1: key questions to ask when appointing a DPO
44	Appendix No. 2: mission statement template to be given by the organisation to the DPO when they take up their post
46	Appendix No. 3: the DPO designation form
51	Appendix No. 4: Glossary



Introduction .....	3
Key focus 1   Getting started .....	4
Key focus 2   Know your business! .....	7
Key focus 3   Manage your relations .....	13
Key focus 4   Get involved! .....	17
Key focus 5   Always be prepared! .....	23
Key focus 6   Keep working! .....	27
Final thoughts .....	31





Французский надзорный орган CNIL (Commission nationale de l'informatique et des libertés) опубликовал утвержденные им руководства по сертификации Data Protection Officer (DPO). Оба документа применимы к DPO, действующим на территории Франции или говорящим по-французски:

- в руководстве по сертификации DPO приводятся требования и условия для рассмотрения заявлений кандидатов, а также перечислены 17 квалификационных критериев, которым необходимо соответствовать для получения статуса сертифицированного DPO со стороны органов по сертификации, аккредитованных CNIL;
- в руководстве по аккредитации излагаются критерии, которым должны удовлетворять организации, претендующие на статус аккредитованных CNIL органов по сертификации DPO.

## 210 Квалификационные требования CNIL к DPO

### Опыт и обучение:



- профессиональный опыт не менее 2 лет в проектах, мероприятиях или задачах, связанных с миссиями DPO в отношении защиты данных; или
- профессиональный опыт не менее 2 лет, а также обучение не менее 35 часов в области защиты данных.

### Знания и навыки:

1. принципы обработки данных;
2. определение правовой основы для обработки данных;
3. форма и содержание информационных уведомлений субъектов данных;
4. управление и обработка запросов на осуществление прав субъектов данных;
5. правовые основы привлечения к обработке данных;
6. управление передачей данных за пределы ЕЭЗ и ее легализация;
7. разработка и внедрение политик и процедур защиты данных;
8. организация аудитов защиты данных и аспекты участия в них;
9. разработка и ведение реестра обработки данных, документации о нарушениях защиты данных;
10. определение мер защиты данных по проекту и по умолчанию;
11. определение технических и организационных мер безопасности данных;
12. уведомление надзорного органа и коммуникация субъектам о нарушениях безопасности данных;
13. определение необходимости оценки воздействия на защиту данных (DPIA) и проверка ее выполнения;
14. консультирование по анализу воздействия на защиту данных (методология, применимые меры);
15. управление отношениями с надзорными органами и содействие их деятельности;
16. разработка и реализация программ обучения и повышения осведомленности по защите данных;
17. обеспечение подотчетности собственной деятельности.

## 211 Квалификационные требования DPC к DPO

**Guidance on Appropriate Qualifications for a Data Protection Officer (GDPR)**



An Coimisiún um Chosaint Sonraí  
Data Protection  
Commission

Article 37(5) GDPR provides that a Data Protection Officer (DPO):

*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.*

The GDPR does not define the professional qualities required or prescribe the training a DPO should undergo to be qualified to undertake the role. This allows organisations to decide on their DPO's qualifications and for training to be tailored to the context of the organisation's data processing.

The appropriate level of qualifications and expert knowledge should be determined according to the personal data processing operations carried out, the complexity and scale of data processing, the sensitivity of the data processed and the protection required for the data being processed.

For example, where a data processing activity is particularly complex, or where a large volume or sensitive data is involved (i.e. an internet or insurance company), the DPO may need a higher level of expertise and support.

Relevant skills and expertise include:

- ✓ expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR;
- ✓ understanding of the processing operations carried out;
- ✓ understanding of information technologies and data security;
- ✓ knowledge of the business sector and the organisation; and
- ✓ ability to promote a data protection culture within the organisation.

For example, a DPO may need an expert level of knowledge in certain specific IT functions, international data transfers, or familiarity with sector-specific data protection practices such as public sector data processing and data sharing, to adequately perform their duties.

Taking into account the scale, complexity and sensitivity of their data processing operations, organisations should proactively decide on the qualifications and level of training required for their DPO.

Ирландский DPA разработал руководство, в котором описываются требования, которые контролеры должны принимать во внимание при оценке уровня знаний и квалификации, которыми должен обладать их DPO.

Соответствующие навыки и знания включают:

- опыт в области национального и европейского законодательства и практики защиты данных, включая глубокое понимание GDPR;
- понимание выполняемых операций по обработке данных;
- понимание информационных технологий и безопасности данных;
- знание бизнес-специфики и бизнес-процессов;
- способность продвигать культуру защиты данных в организации.

## 212 Руководящие принципы португальского CNPD по оценке работы DPO

Португальский орган по защите данных (CNPD) опубликовал 09.05.2023 руководящие принципы по оценке эффективности работы DPO.

Документ содержит информацию об оценке работников, являющихся DPO, включая разграничение между функциональной и нефункциональной деятельностью, а также обеспечение отсутствия конфликта с функцией DPO при выполнении другой работы. Документ подтверждает, что в отсутствие специального правового регулирования не следует проводить комбинированную оценку задач DPO и задач, не связанных с DPO. Хотя документ направлен на оценку работы DPO в государственном секторе, лежащая в его основе логика может быть распространена и на оценку в частных организациях.



<https://www.cnpd.pt/comunicacao-publica/noticias/epd-consulta-publica-a-decorrer/>

[https://www.cnpd.pt/media/xi5lsevz/2023-04-11\\_incompatibilidade-acumula%C3%A7%C3%A3o-fun%C3%A7%C3%B5es-epd-rai.pdf](https://www.cnpd.pt/media/xi5lsevz/2023-04-11_incompatibilidade-acumula%C3%A7%C3%A3o-fun%C3%A7%C3%B5es-epd-rai.pdf)

## Штраф за потенциальный конфликт интересов при назначении DPO от Управления Баварии по защите данных

Bayerisches Landesamt für  
Datenschutzaufsicht



Ansbach, den 20.10.2016

### Pressemitteilung

#### Datenschutzbeauftragter darf keinen Interessenkonflikten unterliegen

Unternehmen, die personenbezogene Daten verarbeiten, sind unter bestimmten Voraussetzungen zur Bestellung eines Datenschutzbeauftragten gesetzlich verpflichtet. Zum Datenschutzbeauftragten können jedoch nicht Personen bestellt werden, die daneben im Unternehmen noch solche Aufgaben wahrnehmen, die zu Interessenkonflikten mit den Aufgaben eines Datenschutzbeauftragten führen können. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat in einem solchen Fall eine Geldbuße gegen ein Unternehmen ausgesprochen.

Unternehmen und andere Stellen müssen einen Datenschutzbeauftragten bestellen, wenn bei ihnen mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten befasst sind. Zahlreiche Unternehmen erfüllen diese Voraussetzungen. Das Gesetz stellt es Unternehmen und anderen Stellen frei, ob die Funktion des Datenschutzbeauftragten an eine externe Person vergeben wird („externer Datenschutzbeauftragter“) oder aber durch einen Mitarbeiter („interner Datenschutzbeauftragter“) erfüllt wird. Wird ein Mitarbeiter zum Datenschutzbeauftragten bestellt, so darf er jedoch daneben nicht noch für solche Aufgaben zuständig sein, die die Gefahr von Interessenkonflikten mit seiner Funktion als Datenschutzbeauftragter mit sich bringen können.

Eine solche Interessenkollision lag nach Auffassung des BayLDA im Falle eines Datenschutzbeauftragten eines bayerischen Unternehmens vor, der die Position des „IT-Managers“ des Unternehmens bekleidete. Eine derart exponierte Position im Hinblick auf die Datenverarbeitungsprozesse im Unternehmen ist in aller Regel unvereinbar mit den Aufgaben eines Datenschutzbeauftragten. Dies liefe letztlich auf eine Datenschutzkontrolle eines der maßgeblichen zu kontrollierenden Funktionsträger im Unternehmen durch sich selbst hinaus. Eine solche Selbstkontrolle widerspricht der Funktion eines Datenschutzbeauftragten, der gerade eine unabhängige Instanz sein soll, die im Unternehmen auf die Einhaltung des Datenschutzes hinwirkt. Diese Aufgabe kann der Datenschutzbeauftragte nicht erfüllen, wenn er gleichzeitig maßgebliche operative Verantwortung für Datenverarbeitungsprozesse besitzt.

Das BayLDA hatte das Unternehmen auf diesen Umstand hingewiesen und zur Bestellung eines Datenschutzbeauftragten aufgefordert, der keiner derartigen Interessenkollision unterliegt. Das Unternehmen kündigte zwar

**Anschrift**  
Bayerisches Landesamt für Datenschutzaufsicht  
Promenade 27  
91522 Ansbach

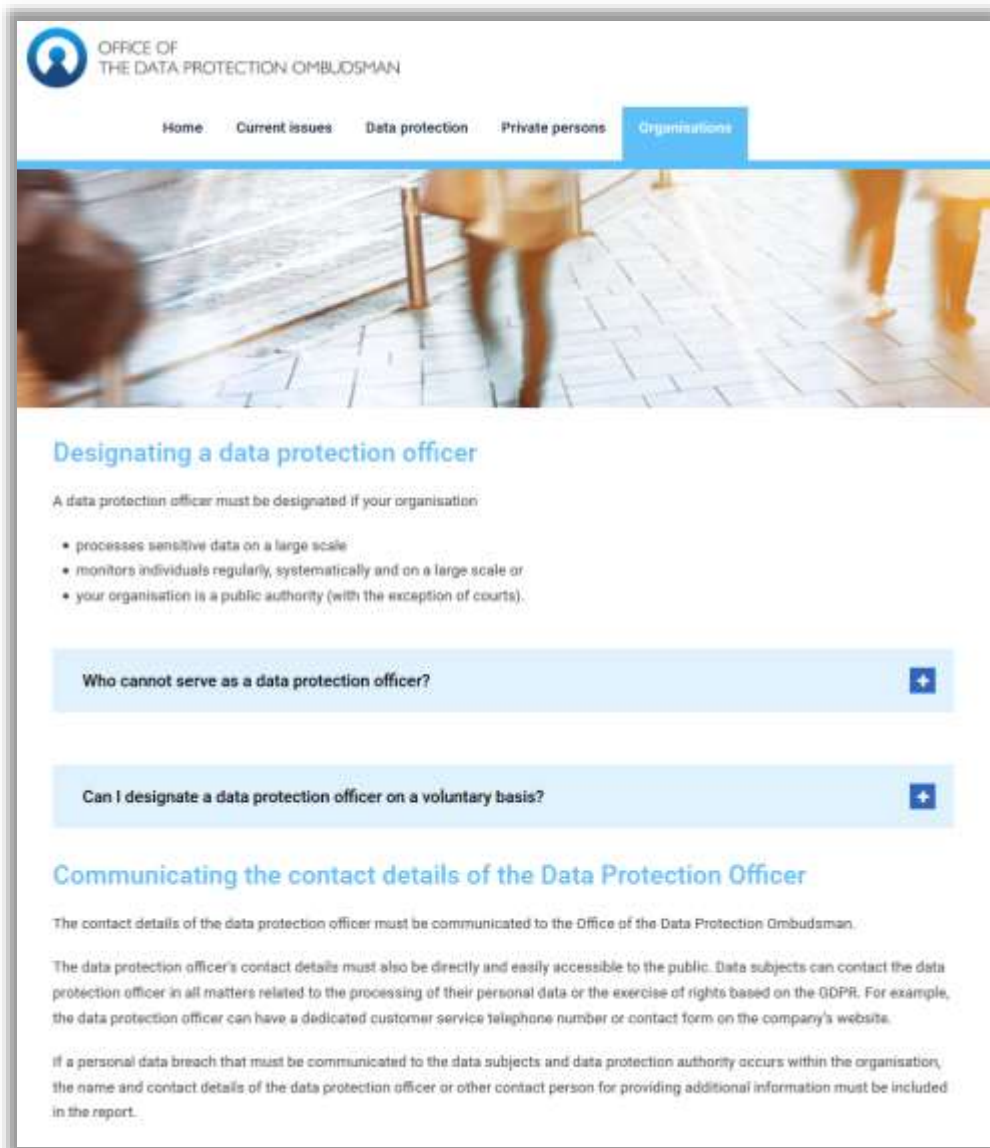
**Telefon** +49 (0) 981 53 1300  
**Telefax** +49 (0) 981 53 98 1300  
**E-Mail** [presse@lda.bayern.de](mailto:presse@lda.bayern.de)  
**Webseite** [www.lda.bayern.de](http://www.lda.bayern.de)

**Öffentliche Verkehrsmittel**  
Bushaltestellen Schlossplatz  
oder Bahnhof der Stadt- und  
Regionalbahnen

Баварский DPA в своем пресс-релизе, опубликованном 20.10.2016, указал о назначении контролеру штрафа за его недостаточное внимание к вопросу назначения DPO и возможного конфликта интересов (когда DPO совмещает выполнение своих задач с другими функциями). Так, DPO не должны «одновременно судить и быть судимыми».

Например, ИТ-менеджеры или системные администраторы, которые не обязательно относятся к высшему руководству организации, но могут принимать решения в отношении обработки данных с использованием информационных систем, не могут быть назначены в качестве DPO.

## 214 Особенности назначения DPO по мнению финского DPA



The screenshot shows the website of the Office of the Data Protection Ombudsman. The page is titled "Designating a data protection officer" and is part of the "Organisations" section. It provides information on when a DPO must be designated and lists criteria for who cannot serve as a DPO. It also includes expandable sections for "Who cannot serve as a data protection officer?" and "Can I designate a data protection officer on a voluntary basis?". Below this, there is a section titled "Communicating the contact details of the Data Protection Officer" which explains that contact details must be communicated to the Ombudsman and be directly accessible to the public. It also states that if a personal data breach occurs, the name and contact details of the DPO must be included in the report.

OFFICE OF THE DATA PROTECTION OMBUDSMAN

Home Current issues Data protection Private persons Organisations

### Designating a data protection officer

A data protection officer must be designated if your organisation

- processes sensitive data on a large scale
- monitors individuals regularly, systematically and on a large scale or
- your organisation is a public authority (with the exception of courts).

Who cannot serve as a data protection officer?

Can I designate a data protection officer on a voluntary basis?

### Communicating the contact details of the Data Protection Officer

The contact details of the data protection officer must be communicated to the Office of the Data Protection Ombudsman.

The data protection officer's contact details must also be directly and easily accessible to the public. Data subjects can contact the data protection officer in all matters related to the processing of their personal data or the exercise of rights based on the GDPR. For example, the data protection officer can have a dedicated customer service telephone number or contact form on the company's website.

If a personal data breach that must be communicated to the data subjects and data protection authority occurs within the organisation, the name and contact details of the data protection officer or other contact person for providing additional information must be included in the report.

DPO не может занимать должность или осуществлять функции, которые будут требовать от него определить цели и методы обработки персональных данных. Определение целей и методов обработки персональных данных является обязанностью контролера.

Конфликт интересов может возникнуть, если, например, CISO или один из топ-менеджеров компании назначен в качестве DPO.

Контактные данные DPO должны сообщаться DPA, а также должны быть явно и легко доступны для всех заинтересованных лиц. Например, у DPO может быть специальный номер телефона службы поддержки клиентов или контактная информация/форма на веб-сайте компании. Если в компании произошла утечка персональных данных, о которой сообщается DPA и затронутым субъектам данных, то в отчет должны быть включены имя и контактные данные DPO для возможности запроса дополнительной информации.

## 215 DPO не может представлять интересы своего нанимателя перед ДРА



HELLENIC DATA PROTECTION AUTHORITY

Athens, 23/1/2020  
Ref.: Gen./Ext./568

### Press release on the representation of controllers before the DPA

~~In view of the fact that~~ in cases of processing of personal data considered by the Authority the controllers often request to be represented by the Data Protection Officer (DPO), the Authority notes the following:

Data Protection Officers are a key component of the new system of personal data governance, as developed under the General Data Protection Regulation 2016/679 (GDPR) and Law 4624/2019 (Government Gazette, A' 137). DPOs assist the controller in complying with the institutional framework for the protection of personal data. However, their opinion is not binding on the controller who has the obligation to take the necessary actions and measures so that that the processing of personal data is in line with the regulatory framework and demonstrate such compliance (accountability). When performing their tasks Data Protection Officers enjoy autonomy and independence, which is not compatible with supporting the lawfulness of the processing of personal data by the controller and may create a conflict of interests with their role as the controller's representative.

The Authority therefore informs the controllers that they are not allowed to be represented by the Data Protection Officer before the Authority. It should be clarified that Data Protection Officers ~~are~~ ~~allowed to~~ be present only if they wish to attend the Authority's meetings.

Communications Department

For more information on DPOs, see "Guidelines for Controllers" ⇨ "Data Protection Officer (DPO)" section on the DPA website [www.dpa.gr](http://www.dpa.gr), as well as the Guidelines on Data Protection Officers ("DPOs") of the Article 29 Working Party (WP. 243 rev. 01 of 05 April 2017).

Греческий ДРА 23 января 2020 года опубликовал заявление о том, что ДРО не имеют права выступать в роли представителя контролера перед надзорными органами, так как это может поставить под угрозу автономию или независимость ДРО.

ДРО оказывают содействие контролеру в создании системы защиты персональных данных, но их мнение не является обязательным для контролера, который обязан предпринять необходимые действия и меры, чтобы обработка персональных данных соответствовала нормативно-правовой базе и демонстрировала такое соответствие (подотчетность).

При выполнении своих задач ДРО пользуются автономией и независимостью, что несовместимо с поддержкой законности обработки персональных данных контролером и может создать конфликт интересов с их ролью представителя контролера.



### D.P.O. – illegittima la richiesta del possesso della certificazione ISO/IEC/27001 quale “titolo abilitante” -TAR Friuli Venezia Giulia, Sez. I<sup>^</sup>, sentenza del 13 settembre 2018, n° 287.

DI LUIGI ROMANO - 20 SETTEMBRE 2018

NEWS

Del 25 maggio 2018, come tutti sanno, è entro in vigore il c.d. GDPR – General Data Protection Regulation – che ha introdotto obblighi stringenti per professionisti e imprese, volti ad elevare il livello di informazione e tutela dei dati personali.

Tra le novità di maggior rilievo vi è senza dubbio quella del c.d. **Data Protection Officer** (D.P.O), il quale, ai sensi dell'art. 37, viene designato dal titolare e dal responsabile del trattamento, "...ogni qualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

#### La decisione del T.A.R.

Esaminata la questione, il Tribunale amministrativo accoglie il ricorso **ritenendo illegittima la richiesta del possesso della certificazione ISO/IEC/27001 quale “titolo abilitante”**. Ad avviso del T.A.R., infatti:

- detto requisito appare ultroneo rispetto ai compiti del DPO, trovando la suddetta certificazione "...prevalente applicazione nell'ambito dell'attività d'impresa" e poiché "...non coglie la specifica funzione di garanzia insita nell'incarico conferito, il cui precipuo oggetto non è costituito dalla predisposizione dei meccanismi volti ad incrementare i livelli di efficienza e di sicurezza nella gestione delle informazioni ma attiene semmai alla tutela del diritto fondamentale dell'individuo alla protezione dei dati personali";
- di contro la "...minuziosa conoscenza e l'applicazione della disciplina di settore restano, indipendentemente dal possesso o meno della certificazione in parola, il nucleo essenziale ed irriducibile della figura professionale ricercata dall'Azienda, il cui profilo, per le considerazioni anzidette, non può che qualificarsi come eminentemente giuridico".

Решением Административного суда региона Фриули – Венеция-Джулия в Италии (TAR Friuli Venezia Giulia) от 20.09.2018 №287 признано противоправным требование местного медицинского учреждения к соискателям позиции, обладающей сходным с Data Protection Officer (DPO) функционалом, обладать сертификатом Ведущего Аудитора в соответствии со стандартом ISO/IEC 27001.



## 217 TAR Puglia – Лессе об ограничениях в аутсорсинге DPO

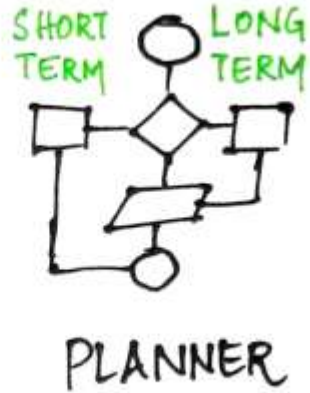


Решением Административного суда региона Апулия – Лечче в Италии (TAR Puglia – Lecce) от 13.09.2019 №182 указано, что при аутсорсинге функции DPO посредством заключения контролером договора со сторонней компанией внешний DPO должен быть работником нанятой компании. Другими словами, невозможно нанять компанию в качестве внешнего DPO и позволить этой компании также нанять субподрядчика для выполнения этой роли.

<https://www.giustizia->

[amministrativa.it/portale/pages/istituzionale/visualizza?nodeRef=&schema=tar\\_le&nrg=201900182&nomeFile=201901468\\_01.html&subDir=Provvedimenti](https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza?nodeRef=&schema=tar_le&nrg=201900182&nomeFile=201901468_01.html&subDir=Provvedimenti)

218 Девять ролевых моделей лидерства для DPO





### “TO BE COMPLIANT”

- What else could my purpose be?
- Data Protection is a **legal issue**
- A necessary evil
- Siloed
- “Defensible position”
- Risk-based: business risks
- Generic policies and procedures
- Shoe string budget
- Resisted and feared



### “ENABLING THE BUSINESS”

- Cultivated a purpose beyond compliance
- Data Protection is a **business imperative**
- Walks the talk
- Collaborative
- Risk-based: risks to individuals
- Embraced by the business
- Tailored ways of working
- Responsibilities embedded in functions & departments
- Data protection compliance is factored into business budgets



DPO перед  
погружением в  
бизнес-процессы  
компании

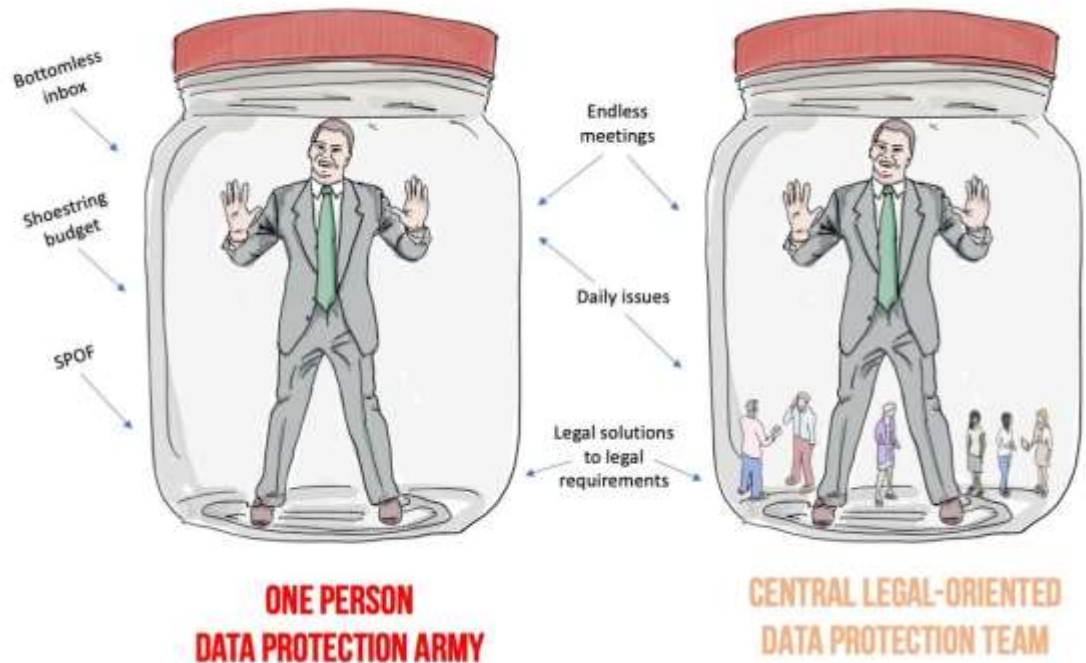
VS.

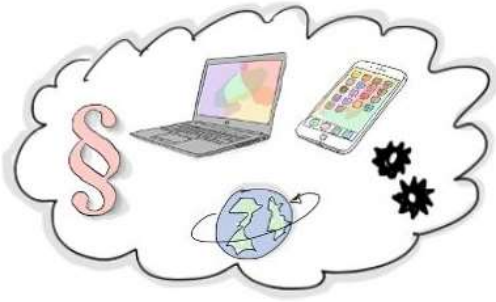
DPO,  
разобравшийся в  
бизнес-процессах  
компании





## 223 Проблемы создания и работы команды DPO





1 Relevant data protection topics/issues

Power/Influence	High	Watch	Keep satisfied	Constant active management
	Some		Keep on side	
	No	Ignore	Keep informed	
		No	Some Interest	High

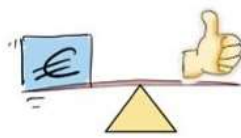
2 Understanding audiences and their needs



3 A huge dose of imagination and creative thinking

Task	Start	Responsible	Target group	Phase	Project	Initiation	Analysis	Design	Implementation	Final Review	Completion
Task 1	2023-01-01	John Doe	Internal	Phase 1	Project A	Initiation	Analysis	Design	Implementation	Final Review	Completion
Task 2	2023-01-01	Jane Smith	External	Phase 2	Project B	Initiation	Analysis	Design	Implementation	Final Review	Completion

4 Engagement plan



5 Business case



Budget



6 Buy-in and approval

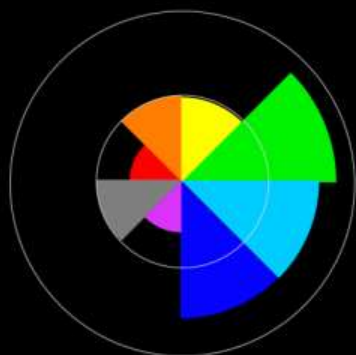




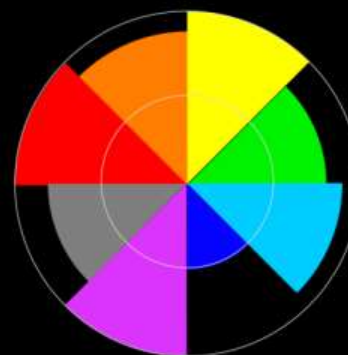
# Internal DPO vs. External DPO



Internal DPO / External DPO



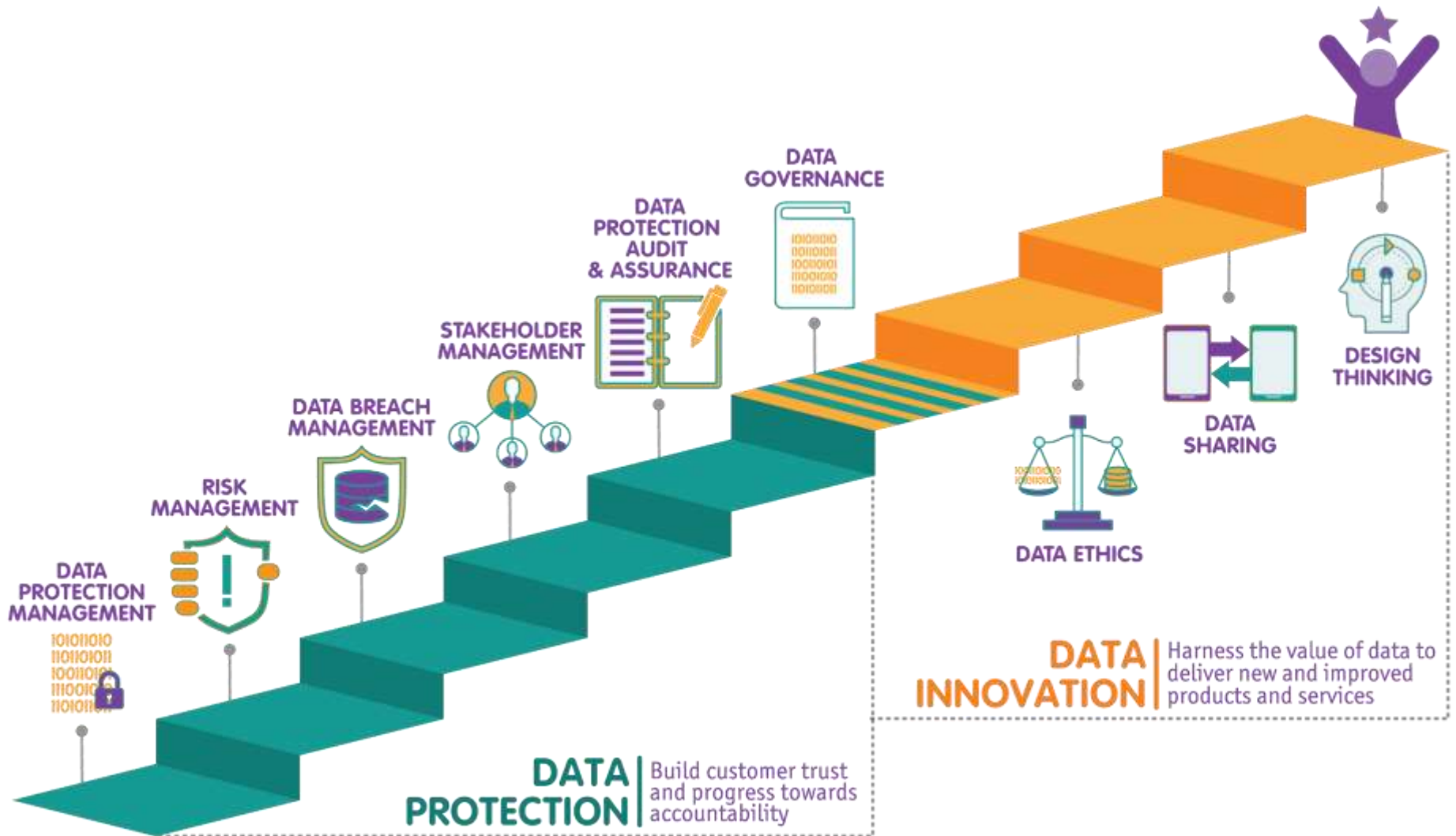
or ...



## Legend

- Independence
- No conflict of interest
- Authority
- Trust
- Involvement
- Financial efficiency
- Competence
- Risks and Liability

## Описание компетенций и дорожной карты развития DPO от Комиссии по защите персональных данных Сингапура





## Краткая характеристика каждой из ступеней развития компетенций DPO

Каждая из ступеней развития компетенций DPO может быть кратко охарактеризована следующим образом:

- 1. управление защитой данных** – разработка и внедрение политик и процедур управления защитой персональных данных организации в соответствии с применимым законодательством и лучшими практиками;
- 2. управление ИТ-рисками** – эффективное прогнозирование и оценка существующих и потенциальных ИТ-рисков, которые влияют на работу и (или) прибыльность деятельности организации, а также на разработку и внедрение общеорганизационных стратегий и процессов для снижения рисков, связанных с обработкой персональных данных;
- 3. управление нарушениями безопасности данных** – выявление инцидентов в сфере кибербезопасности и утечек данных, определение фактических обстоятельств и последствий нарушений, принятие мер для устранения или уменьшения масштаба последствий инцидентов и утечек, эффективные коммуникации о нарушениях в адрес соответствующих заинтересованных лиц;
- 4. управление заинтересованными сторонами** – управление ожиданиями и потребностями сторон (стейкхолдеров), заинтересованных в состоянии защищенности персональных данных, с учетом требований и целей организации в целом;
- 5. аудит и комплаенс** – организация эффективного внешнего и внутреннего мониторинга и контроля (в том числе путем реализации процедур информирования о нарушениях и проведения служебных расследований) за соблюдением применимых норм в области персональных данных;
- 6. управление данными** – разработка и внедрение в деятельность организации руководящих принципов и правил надлежащей обработки персональных данных на различных этапах их жизненного цикла, а также предоставление активных рекомендаций в отношении обработки данных и устранения утечек данных в различных сложных, неоднозначных или многогранных контекстах;
- 7. этика данных** – применение этических принципов<sup>1</sup> при формировании процессов обработки персональных данных в контексте деятельности организации;
- 8. обмен данными** – умение адекватно определять ценность персональных данных для достижения конкурентного преимущества и (или) целей организации;
- 9. навыки дизайн-мышления** – руководство методологическими и процессными аспектами дизайн-мышления<sup>2</sup> для решения конкретных задач организации и управление заинтересованными сторонами на этапах определения проблемы, исследования, формирования идеи и ее осуществления.

<sup>1</sup> См., например, отчет «Этика данных: проявление морали в технологиях» Всемирной федерации рекламодателей (World Federation of Advertisers, WFA) - <https://wfanet.org/leadership/data-ethics>

<sup>2</sup> См., например, книгу Герберта Саймона «Науки об искусственном» (The Sciences of the Artificial) - [https://monoskop.org/images/9/9c/Simon\\_Herbert\\_A\\_The\\_Sciences\\_of\\_the\\_Artificial\\_3rd\\_ed.pdf](https://monoskop.org/images/9/9c/Simon_Herbert_A_The_Sciences_of_the_Artificial_3rd_ed.pdf)



В августе 2018 года стало известно, что генеральный секретарь Департамента по вопросам занятости и социальной защиты (Department of Employment Affairs and Social Protection - DEASP) распорядился внести изменения в политику Департамента в отношении конфиденциальности в Интернете и удалить упоминание о сборе биометрических данных. Изменения были внесены, когда лицо, ответственное за защиту персональных данных (Data Protection Officer – DPO) в Департаменте, находилось в отпуске, а его дальнейшие показания о свидетельствуют о несогласии DPO с такими изменениями и что они не обсуждались с ним.

Тогда же ирландский надзорный орган (Data Protection Commission - DPC), по жалобе НКО "Digital Rights Ireland" от имени Карлина Лиллингтона (Karlin Lillington) – журналиста издания "Irish Times", инициировал расследование о возможном нарушении статьи 38 GDPR в виде вмешательства в работу DPO со стороны его нанимателя. В августе 2019 года стало известно, что в предварительных результатах расследования DPC был зафиксирован факт незаконного вмешательства руководства DEASP в работу собственного DPO, и теперь Департаменту грозит штраф размером до €1,000,000.

## 230 Штраф за назначение ненадлежащего лица в качестве DPO

Бельгийский надзорный орган (l'Autorité de protection des données) в апреле 2020 года оштрафовал компанию Proximus SA за нарушение ст. 32 и 38(6) GDPR на сумму в €50,000.

### Причина:

Назначение в качестве DPO директора департамента внутреннего аудита, управления рисками и комплаенса признано ненадлежащей практикой, что лишило DPO независимости в принятии решений и породило конфликт интересов, хотя ранее в Руководстве WP29 прямо указывалось, что при выборе DPO не стоит рассматривать такие руководящие позиции как CEO, COO, Head of Marketing, Head of HR или Head of IT. Поэтому широко распространённой практикой стало назначение в качестве DPO лиц, занимающих позиции Head of Compliance или Head of Legal.

### Доводы DPA:

- нарушение порядка разграничения полномочий, отсутствие процедуры разграничения полномочий и доказательств фактической независимости DPO в принятии решений;
- DPO не принимал участие в обсуждениях результатов анализа рисков, а только информировался исходя из действовавшей в компании RACI-матрицы (нарушение ст. 25 и 38(1) GDPR), но суд не согласился с этим доводом DPA;
- DPO был руководителем департамента аудита, рисков и комплаенса, тогда как роль руководителя департамента не совместима с ролью DPO – руководитель структурного подразделения принимает решения в отношении работников (своих подчиненных), а также определяет цели, средства и способы обработки персональных данных, что породило конфликт интересов в отношении функции DPO (нарушение ст.38(6) GDPR). Кроме того, объединение обозначенных функций в одной позиции может повлиять на конфиденциальность персональных данных.
- DPO недостаточно интенсивно участвовал в расследовании и ликвидации нарушений безопасности персональных данных (data breach).

## 231 Штрафы за нарушения в назначении и работе DPO

**Кто:** Commission nationale pour la protection des données (Люксембург)

**Кого:** три неизвестных компании

**Когда:** 2021.10

**За что:** нарушение ст. 37(7), 38(1)-(3), 39(1) а) и b) GDPR

**Как:** штрафы €13,200, €18,000, €15,400

**Причина:** одну из компаний попытались уличить в нарушении ст.37(5) GDPR – назначать DPO на основании его/ее профессиональных качеств, т.к. DPO должен обладать не менее 3 лет профессионального опыта в области защиты данных. CNPD счёл, что DPO не обладал каким-либо особым опытом в области защиты данных на момент своего назначения, но был назначен потому, что он уже занимал должность «Директора по комплаенсу и юридического отдела». В ответ на это компания направила в CNPD дополнительные документы, подтверждающие, что DPO имеет более 3 лет профессионального опыта в области защиты данных.

Другим нарушением было непривлечение DPO ко всем вопросам, связанным с защитой данных (ст.38(1) GDPR). CNPD считает, что это достигается, если DPO формально и часто участвует в исполнительном комитете, комитетах по координации проектов, комитетах по новым продуктам, комитетах по безопасности или в других комитетах, которые считаются полезными в контексте защиты персональных данных.

Еще одним нарушением было непредоставление DPO необходимых ресурсов (ст.38(2) GDPR). Согласно CNPD, это достигается, если команде DPO выделяется как минимум один эквивалент полной занятости (ЭПЗ - FTE), т.е. один человек, работающий полный рабочий день в качестве DPO, и имеет возможность полагаться на другие подразделения, такие как юридический отдел, ИТ, безопасность и т. д. В ходе проверки было обнаружено, что ресурсы, выделенные группе защиты данных, были приблизительно 0,7 ЭПЗ. Кроме того, не было определено время, отведенное DPO к задаче защиты данных.

Также было обнаружено нарушение обязательства гарантировать, что DPO имеет задачу контролировать соответствие GDPR с политиками контролера (ст.39(1) GDPR). Согласно CNPD, это обязательство достигается, если организация имеет формализованный план контроля защиты данных, в котором определены задачи мониторинга группы DPO. Проверка показала, что у компании были определенные процедуры (например, для ответа на запросы субъектов данных), но не было процедур мониторинга.

<https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-36FR-2021-sous-forme-anonymisee.pdf>

<https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-38FR-2021-sous-forme-anonymisee.pdf>

<https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-40FR-2021-sous-forme-anonymisee.pdf>

## Штраф Facebook за неназначение DPO и неуведомление надзорного органа

Bloomberg the Company & Its Products | Bloomberg Anywhere Remote Login | Bloomberg Terminal Demo Request

**Bloomberg**

Business

### Facebook's Tiny Privacy Fine Is a 'Warning,' Watchdog Says

By [Stephanie Bodoni](#)  
13 февраля 2020 г., 12:18 GMT+3 Updated on 13 февраля 2020 г., 17:37 GMT+3

- Hamburg privacy watchdog levies symbolic EU\$1,000 penalty
- EU's new privacy rules give authorities higher fining powers

LISTEN TO ARTICLE  
▶ 2:00

SHARE THIS ARTICLE  
 f Share  
 t Tweet  
 in Post  
 e Email

**In this article**

FB  
FACEBOOK INC-A  
217.49 USD  
▼ -0.31 -0.14%

Facebook Inc.'s German unit was handed a fine of 51,000 euros (\$55,500) for failing to properly nominate a data protection officer for its local office, a penalty privacy regulators said should still serve as a "warning" to others.

While the punishment seems tiny for the social network giant, it targets the German unit and not the "billion-dollar parent company," the data protection authority in Hamburg, Germany, said in its 2019 annual report published on Thursday.

"This case should be a clear warning to all other companies: naming a data protection officer and telling the regulator about it are duties," which the data protection authority takes seriously, the watchdog said in the report. "Even smaller violations like these can lead to substantial penalties."

The penalty was levied under the European Union's new privacy rules, which took effect in May 2018. The General Data Protection Regulation, or GDPR, gives EU data protection authorities for the first time equal powers to fine companies as much as 4% of global annual sales for the most serious violations of people's personal data.

**Кто:** Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Германия)

**Кого:** Facebook Inc.

**Когда:** 2020.02

**За что:** нарушение ст. 37 GDPR

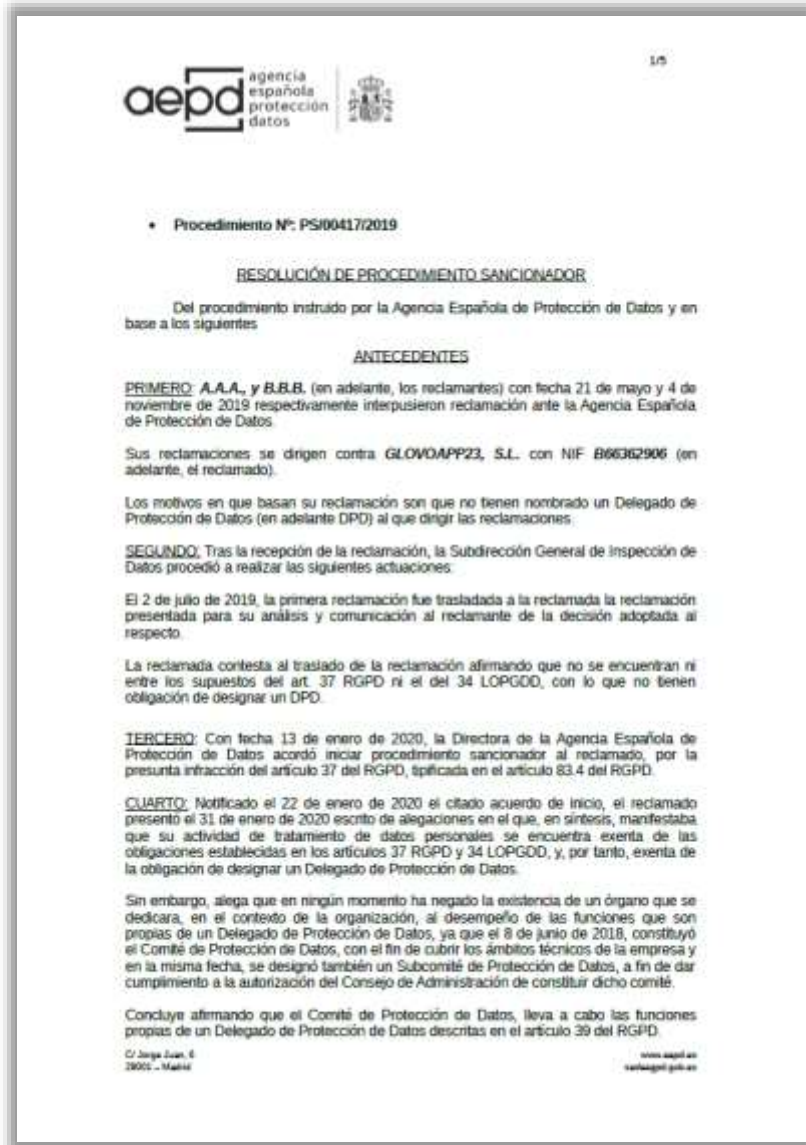
**Как:** штраф €51,000

**Причина:** немецкое подразделение Facebook Inc. не назначило DPO и не сообщило его контактные данные немецкому надзорному органу. В свою защиту Facebook утверждал, что его DPO был назначен в Ирландии, и что он будет исполнять свою функцию в отношении всех европейских подразделений Facebook. Немецкое DPA подчеркнуло, что Facebook заранее не уведомлял надзорный орган о упомянутой номинации DPO.

На размер штрафа положительно повлияла немедленная реакция Facebook на предписание и оперативное предоставление контактных данных DPO.



## Штраф за неназначение DPO и делегирование его полномочий комитету по защите данных



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Glovoapp23 SL

**Когда:** 2020.06

**За что:** нарушение ст. 37 GDPR

**Как:** штраф €25,000

**Причина:** двое заявителей утверждали, что компания не назначила DPO, которому они могли бы направить свои запросы. При этом компания утверждала об отсутствии у нее обязательства назначать DPO, поскольку осуществляемая деятельность по обработке данных не подпадает под требование ст.37(1) GDPR, а функции DPO выполнял комитет по защите данных компании.

## 234 Выговор за неназначение DPO и непубликацию его контактных данных

Decision exercising corrective powers made under the Data Protection Act 2018

### Inquiry into the Pre-Hospital Emergency Care Council

(IN-22-2-1)  
Date of Decision: 03 May 2022

The Data Protection Commission (DPC) commenced this own-volition inquiry as a result of a monitoring and enforcement exercise carried out pursuant to the tasks of a supervisory authority contained in Article 57 of the GDPR.


The DPC sought to monitor and enforce the application of the GDPR concerning the designation of a Data Protection Officer (DPO) by organisations. The designation of a DPO and related obligations of data controllers are contained in Article 37 of the GDPR. The Pre-Hospital Emergency Care Council was identified as an apparent public sector organisation that may be required to designate a DPO, publish the details of the DPO and communicate them to the DPC as the supervisory authority.

The Pre-Hospital Emergency Care Council (PHECC) was one of many public sector organisations contacted during the monitoring and enforcement exercise. PHECC did not respond to any correspondence issued to it. There was no record in the DPC of the PHECC having communicated its DPO details to the DPC. In addition, there were no contact details for a DPO available on the PHECC website.

This inquiry was commenced to establish whether the PHECC was required to designate a DPO pursuant to Article 37(1) of the GDPR and whether the PHECC had done so. In addition, the inquiry sought to establish whether the PHECC infringed Article 37(7) of the GDPR concerning the publication of the DPO contact details and the communication of contact details to the DPC. The inquiry was also commenced to establish whether the PHECC infringed Article 31 of the GDPR by failing to cooperate, on request, with the DPC in the performance of its tasks.

The Decision found that the PHECC had infringed the following provisions of the GDPR:

- Article 37(1) of the GDPR, which requires inter alia that public sector controllers designate a data protection officer. The PHECC infringed Article 37(1) by failing to designate a data protection officer for the organisation.
- Article 37(7) of the GDPR was infringed by the PHECC by failing to publish the contact details of a data protection officer and failing to communicate the contact details to the supervisory authority.
- Article 31 of the GDPR requires controllers to cooperate with the supervisory authority, on request, when carrying out its tasks pursuant to Article 57 of the



An Coimisiún um  
Chosaint Sonraí  
Data Protection  
Commission

**Кто:** Data Protection Commission (Ирландия)

**Кого:** Совет по оказанию неотложной помощи на догоспитальном этапе ("PHECC")

**Когда:** 2022.05

**За что:** нарушение ст. 31, 37(1), 37(7) GDPR

**Как:** выговор

**Причина:** PHECC допустил нарушений GDPR:

- неназначение DPO;
- непубликация контактных данных DPO;
- нежелание сотрудничать с DPC (игнорирование запросов).

При этом отказ PHECC сотрудничать с DPC был квалифицирован как непреднамеренный.

### Pressemitteilung

711.412.1

5. November 2019

#### Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft

Am 30. Oktober 2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) erlassen.

Bei Vor-Ort-Prüfungen im Juni 2017 und im März 2019 hat die Aufsichtsbehörde festgestellt, dass das Unternehmen für die Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendete, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen. Personenbezogene Daten von Mieterinnen und Mietern wurden gespeichert, ohne zu überprüfen, ob eine Speicherung zulässig oder überhaupt erforderlich ist. In begutachteten Einzelfällen konnten daher teilweise Jahre alte private Angaben betroffener Mieterinnen und Mieter eingesehen werden, ohne dass diese noch dem Zweck ihrer ursprünglichen Erhebung dienten. Es handelte sich dabei um Daten zu den persönlichen und finanziellen Verhältnissen der Mieterinnen und Mieter, wie z. B. Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankensicherungsdaten sowie Kontoauszüge.

Nachdem die Berliner Datenschutzbeauftragte im ersten Prüftermin 2017 die dringende Empfehlung ausgesprochen hatte, das Archivsystem umzustellen, konnte das Unternehmen auch im März 2019, mehr als eineinhalb Jahre nach dem ersten Prüftermin und neun Monate nach Anwendungsbeginn der Datenschutz-Grundverordnung weder eine Bereinigung ihres Datenbestandes noch rechtliche Gründe für die fortdauernde Speicherung vorweisen. Zwar hatte das Unternehmen Vorbereitungen zur Beseitigung der aufgefundenen Missstände getroffen. Diese Maßnahmen hatten jedoch nicht zur Herstellung eines rechtmäßigen Zustands bei der Speicherung personenbezogener Daten geführt. Die Verhängung eines Bußgeldes wegen eines

Pressesprecherin: Dalia Kues  
Geschäftsstelle: Cristina Vecchi  
E-Mail: [presse@datenschutz-berlin.de](mailto:presse@datenschutz-berlin.de)

Friedrichstr. 219    Tel: 030 13889 - 900  
10969 Berlin        Fax: 030 2156050



**Кто:** BDI Berliner (Германия)

**Кого:** дочерняя компания неназванной ритейл-группы

**Когда:** 2022.09

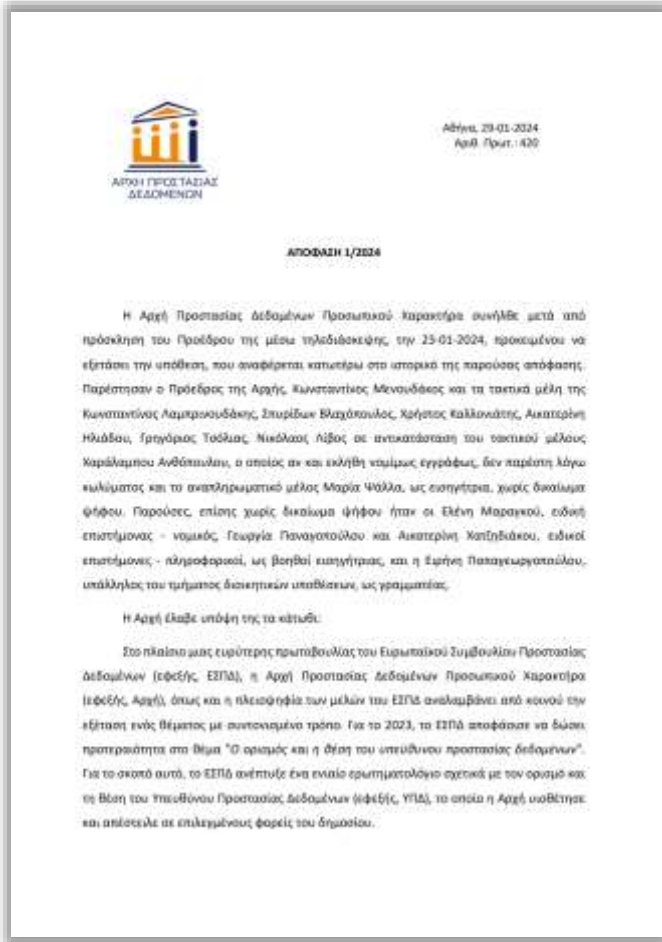
**За что:** нарушение ст.38(6) GDPR

**Как:** штраф €525,000 после первоначального предупреждения, вынесенного компании в 2021 году

**Причина:** компания назначила DPO для независимого контроля решений, принятых им же в другом качестве. Данное лицо являлось управляющим директором двух сервисных компаний в рамках одной группы, которые обрабатывали персональные данные от имени компании, для которой оно являлось DPO, при обслуживании клиентов и выполнении заказов.

В связи с этим DPA уточнил, что DPO должен был следить за соблюдением законодательства о защите данных сервисными компаниями, которыми он руководил как управляющий директор.

## 236 Штраф за незаполнение анкеты надзорного органа со стороны DPO



**Κτο:** Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

**Κογο:** Δήμος Αθηναίων (муниципалитет Αφιν)

**Κοгда:** 2024.02

**За что:** нарушение ст. 31, 37, 38, 39 GDPR

**Как:** штраф €5,000

**Причина:** Греческое управление по защите данных (HDPA) в рамках изучения темы "Определение и должность DPO" направило ряду организаций унифицированную анкету. DPO муниципалитета Афин не ответил на анкету в установленный срок. HDPA повторно отправил анкету – и снова DPO не ответил. После истечения срока DPO попытался заполнить анкету, но безуспешно, поскольку вышеуказанная ссылка была деактивирована HDPA. После того как DPO связался с HDPA, ссылка была восстановлена, но DPO опять не представил анкету.

После этого HDPA вызвал контролера на дачу объяснений. DPO связался с HDPA по телефону и сообщил, что по ошибке не смог ответить на вопросник из-за технических проблем, и обязался заполнить и представить его немедленно. После этого DPA Греции вновь активировал ссылку на отправку анкеты, и DPO в итоге отправил анкету. Позже DPO еще раз заявил, что причиной задержки ответа стали технические проблемы с веб-сайтом, на котором размещалась анкета, которые не позволили отправить анкету даже после нескольких попыток.

[https://www.dpa.gr/sites/default/files/2024-02/1\\_2024%20anonym.pdf](https://www.dpa.gr/sites/default/files/2024-02/1_2024%20anonym.pdf)

[https://gdprhub.eu/index.php?title=HDPA\\_\(Greece\)\\_-\\_1/2024](https://gdprhub.eu/index.php?title=HDPA_(Greece)_-_1/2024)

## DPO может быть уволен, если больше не обладает необходимыми профессиональными качествами



21 OCTOBRE 2022

### Base de jurisprudence

Ariane Web: Conseil d'État 459254, lecture du 21 octobre 2022.  
ECLI:FR:CECHR:2022:459254.20221021  
Decision n° 459254

Conseil d'État

N° 459254  
ECLI:FR:CECHR:2022:459254.20221021  
Publié au recueil Lebon

10ème - 9ème chambres réunies

Mme Isabelle Lemesle, rapporteur  
Mme Esther de Moustier, rapporteur public  
SCP FABIANI, LUC-THALER, PINATEL, avocats

Lecture du vendredi 21 octobre 2022

REPUBLIQUE FRANÇAISE

AU NOM DU PEUPLE FRANÇAIS

Vu la procédure suivante :

Par une requête sommaire, un mémoire complémentaire et trois mémoires en réplique, enregistrés les 8 décembre 2021, 9 mars, 2 juin, 15 juillet et 20 septembre 2022 au secrétariat du contentieux du Conseil d'Etat, Mme A... C... demande au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir la décision du 8 octobre 2021 de la présidente de la Commission nationale de l'informatique et des libertés (CNIL) clôturant sa plainte dirigée contre la société ... ;

2°) de mettre à la charge de la société ... la somme de 3 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Государственный совет Франции 21.10.2022 подтвердил решение французского надзорного органа ("CNIL") о функциях DPO, согласно которому компания, уволившая заявителя, который работал ответственным лицом по защите персональных данных (Data Protection Officer – "DPO"), не нарушила ст.38(3) GDPR, касающуюся функций и независимости DPO.

В своем решении Государственный совет заявил, что положения GDPR, направленные на сохранение функциональной независимости DPO, не предназначены для регулирования общих трудовых отношений между контроллером или процессором и его работниками, и что работник, выполняющий функции DPO в компании, может быть уволен, если он больше не обладает профессиональными качествами, необходимыми для выполнения своих обязанностей, или не выполняет их в соответствии с GDPR, приведя в качестве примера непредставление DPO запрошенной его нанимателем плана по обеспечению привасу-комплаенса в компании или неспособность DPO отвечать на запросы работников.

Государственный совет взыскал с истца (бывшего DPO) сумму в €1,000 в качестве судебных издержек.

## Федеральный административный суд Австрии постановил, что субъекты данных не могут добиваться назначения DPO

**Gericht**  
Bundesverwaltungsgericht

**Entscheidungsdatum**  
03.08.2023

**Geschäftszahl**  
W101 2258430-1

**Spruch**  
  
W101 2258430-1/33E

IM NAMEN DER REPUBLIK!

Das Bundesverwaltungsgericht hat durch die Richterin Dr. Christine AMANN als Vorsitzende und die fachkundige Laienrichterin Mag. Viktoria HAIDINGER als Beisitzerin sowie den fachkundigen Laienrichter Mag. Thomas GSCHAAR als Beisitzer über die Beschwerde von XXXX, vertreten durch die RAe Dr. Kurt Bayr & Dr. Marco Rovagnati, gegen den Spruchteil 3. des Bescheides der Datenschutzbehörde vom 06.07.2022, GZ. D124.4072 2022-0.61.103, nach Durchführung einer mündlichen Verhandlung am 28.04.2023 zu Recht erkannt:

A)

I. Gemäß § 28 Abs. 2 VwGVG iVm § 24 Abs. 1 und Abs. 5 DSGVO idGF wird der Beschwerde hinsichtlich der behaupteten Verletzung im Recht auf Geheimhaltung mit der Maßgabe stattgegeben, dass der angefochtene Spruchteil diesbezüglich zu lauten hat:

„3.1. Der Datenschutzbeschwerde wird teilweise stattgegeben und es wird festgestellt, dass der Beschwerdegegner den Beschwerdeführer dadurch in seinem Recht auf Geheimhaltung verletzt hat, indem er einerseits das E-Mail samt Schreiben vom 08.02.2021 an folgende E-Mail-Adressen übermittelt hat, sodass dieses insgesamt 10 Personen offengelegt wurde: XXXX, XXXX, XXXX, XXXX, XXXX, XXXX,“

und

indem er andererseits dieses E-Mail samt Schreiben im Personalakt des Beschwerdeführers bei der Pädagogischen Hochschule XXXX von XXXX ablegen hat lassen, sodass es noch weiteren Personen offengelegt wurde.“

II. Gemäß § 28 Abs. 2 VwGVG iVm § 24 Abs. 1 und Abs. 5 DSGVO idGF wird die Beschwerde hinsichtlich der behaupteten weiteren Verletzung im Recht auf Auskunft mit der Maßgabe als unbegründet abgewiesen, dass der angefochtene Spruchteil diesbezüglich zu lauten hat:

„3.2. Im Übrigen wird die Datenschutzbeschwerde als unbegründet abgewiesen.“

B)

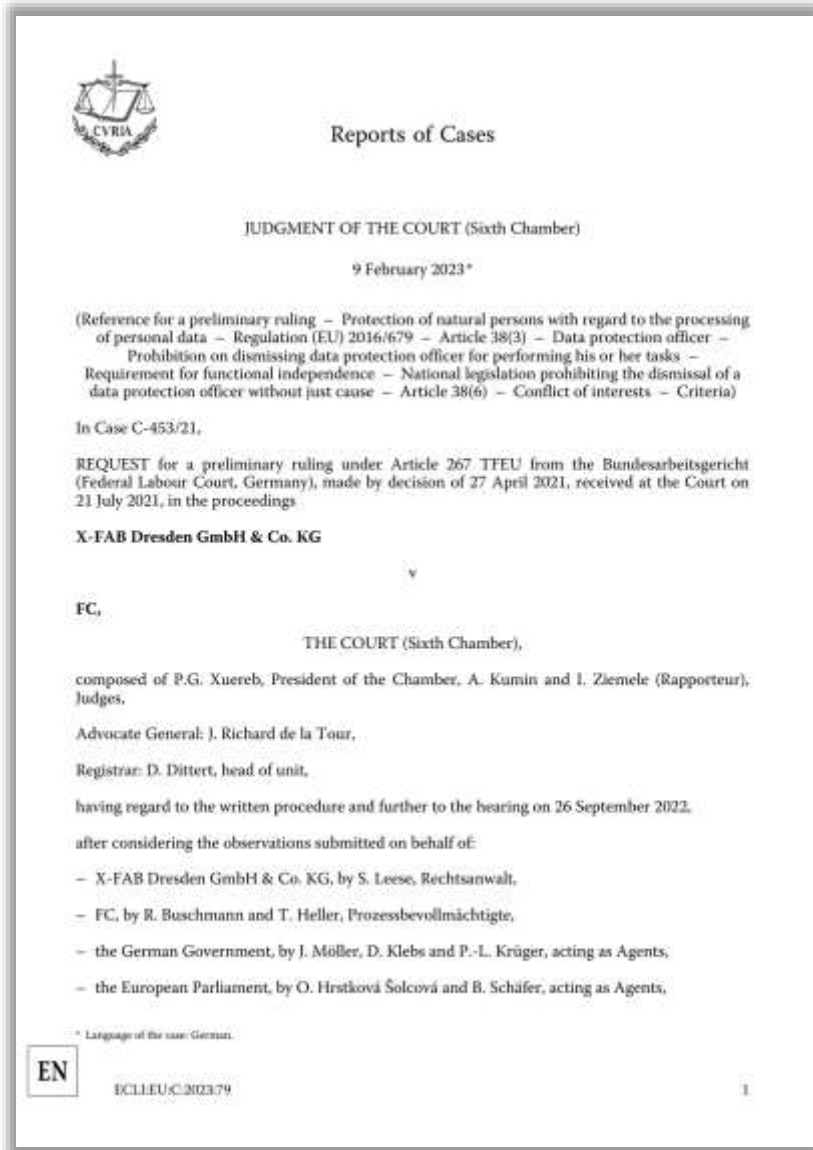
Die Revision ist gemäß Art. 133 Abs. 4 B-VG nicht zulässig.

◇ Федеральный административный суд (BVwG) в своем решении от 03.08.2023 г. частично подтвердил решение австрийского органа по защите данных (DSB), касающееся права доступа, права на неприкосновенность частной жизни и права требовать назначения ответственного за защиту данных (DPO) заявителя в соответствии с GDPR.

◇ По словам заявителя, его право на доступ было нарушено ответчиком - неназванным университетом. Университет направил электронное письмо о предполагаемом нарушении заявителем своих служебных обязанностей в несколько департаментов. Кроме того, когда заявитель запросил доступ к своим данным, он получил документ объемом более 800 страниц, в котором не было ни одной ссылки на него. Кроме того, BVwG заявила, что, по мнению заявителя, ответ на запрос о доступе должен был дать DPO, а не декан университета.

◇ Суд установил, что университет нарушил право заявителя на конфиденциальность, отправив вышеупомянутое электронное письмо и письмо, которое было раскрыто другим лицам. В отношении рассмотрения вопроса о назначении DPO, суд постановил, что, хотя назначение DPO представляет собой обязанность контроллера данных, оно не влечет за собой права субъекта данных требовать назначения DPO. В свете вышеизложенного BVwG частично удовлетворил жалобу и отклонил апелляцию.

## CJEU: совмещение позиции председателя рабочего совета и DPO ведет к конфликту интересов



Европейский суд (CJEU) 09.02.2023 постановил по делу C-453/21 X-Fab Dresden GmbH & Co. KG, что каждое государство-член может устанавливать более конкретные правила, касающиеся увольнения DPO, при условии, что эти правила совместимы с законодательством ЕС и GDPR. CJEU также постановил, что "конфликт интересов", согласно статье 38(3) GDPR, может иметь место, когда на DPO возложены другие задачи или обязанности, в результате чего он/она определяет цели и методы обработки персональных данных от имени обработчика/контролера.

Ранее субъект данных был сотрудником контролера, компании X-FAB (производство полупроводников), и занимал в компании две должности: он был председателем рабочего совета и DPO в X-Fab и других компаниях той же группы предприятий. Однако 01.12.2017 субъект данных был отстранен от исполнения своих обязанностей в качестве DPO по просьбе DPA земли Тюринген (TLfDI) (Германия). В качестве меры предосторожности другие предприятия также приняли решение о его увольнении на основании второго предложения ст.38(3) GDPR, которое стало применимым за прошедший период.

<https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-453/21>

[https://gdprhub.eu/index.php?title=CJEU - C-453/21 - X-Fab Dresden GmbH %26 Co. KG](https://gdprhub.eu/index.php?title=CJEU_-_C-453/21_-_X-Fab_Dresden_GmbH_%26_Co._KG)

## EDPB и национальные DPA опрашивают DPO для выявления возможных нарушений требований GDPR

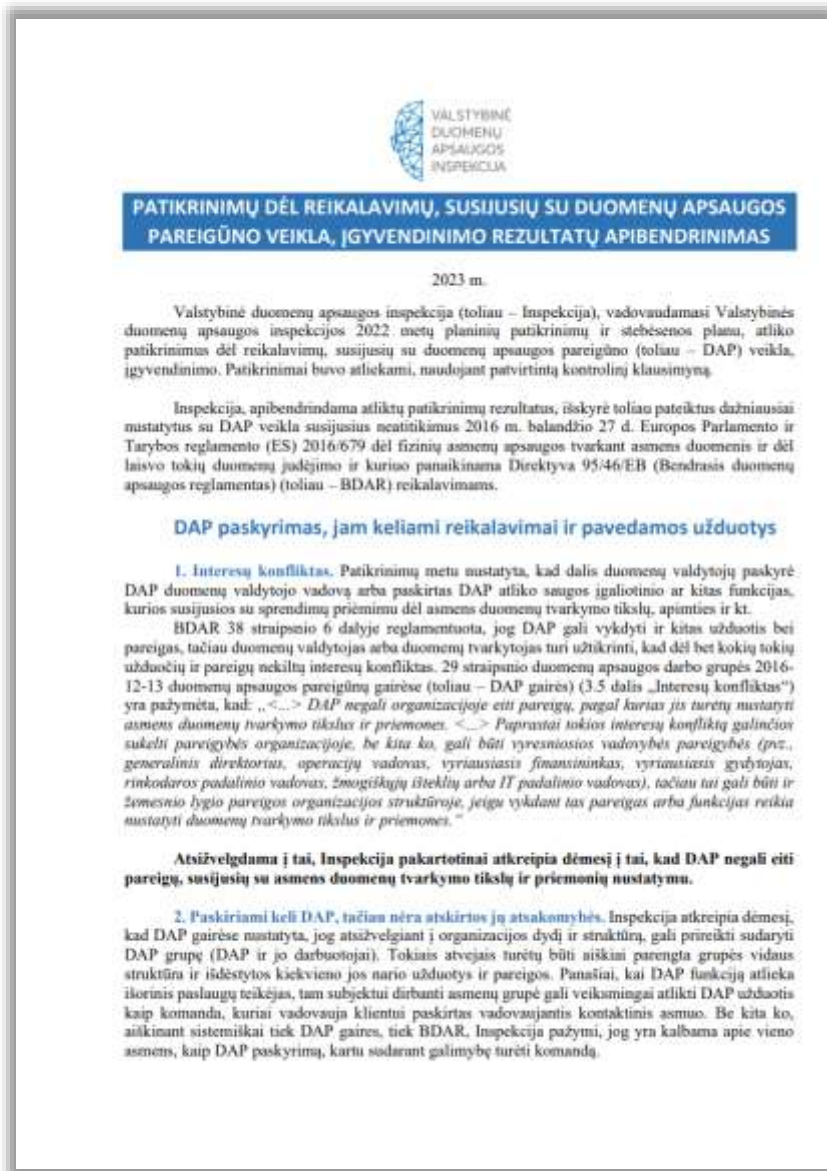


Европейский совет по защите данных (EDPB) 15.03.2023 объявил о начале скоординированных с национальными надзорными органами (DPA) правоприменительных действий на 2023 год, которые будут посвящены вопросам надлежащего назначения ответственных за защиту данных (DPO) согласно ст.37-39 GDPR, а также предоставления DPO ресурсов, необходимые для выполнения их задач. Планируются следующие шаги:

- ◇ анкетирование DPO для выявления возможных нарушений требований GDPR;
- ◇ инициирование официальных расследований или корректирующих действий в случае выявления нарушений.

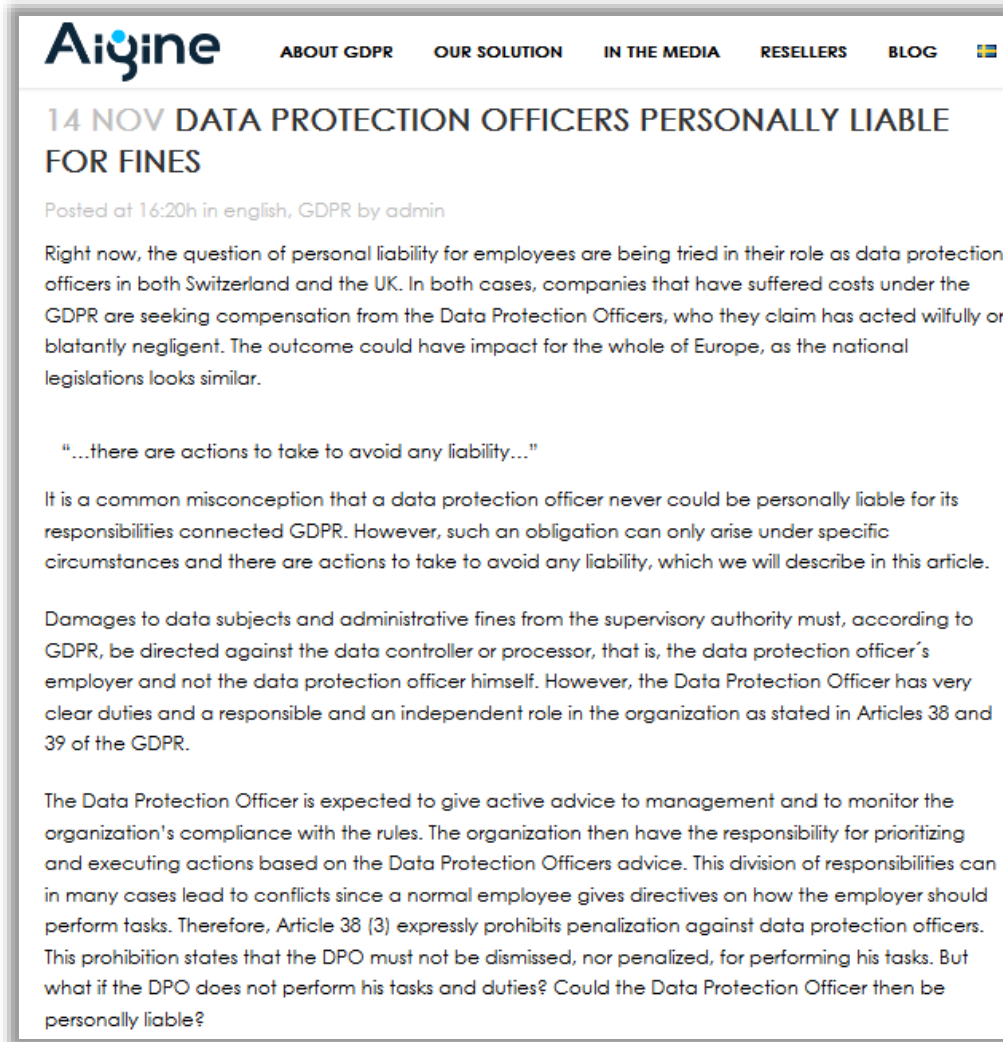


## Литовская VDAI опубликовала результаты проверок деятельности DPO



Государственная инспекция по защите данных Литвы ("VDAI") 18.04.2023 опубликовала обобщенные результаты проверок в 2022г. деятельности офицеров по защите данных ("DPOs") с целью выявления соответствия GDPR. Среди наиболее распространенных нарушений было выявлено следующее:

- ◇ конфликт интересов, когда DPO выполняют функции менеджеров структурных подразделений и определяют цели и средства обработки персональных данных;
- ◇ отсутствие документирования обязанностей/функций DPO и их команды;
- ◇ работники не были должным образом проинформированы о назначенном DPO и его функциях, чтобы они могли легко связаться с ним по любым вопросам, касающимся GDPR;
- ◇ при смене DPO в организации информация о таком изменении не была опубликована;
- ◇ DPO не проводили периодические оценки и аудиты соблюдения GDPR в организации и не информировали своего нанимателя об их результатах.



The screenshot shows a blog post from Aigine. The header includes the Aigine logo and navigation links: ABOUT GDPR, OUR SOLUTION, IN THE MEDIA, RESELLERS, BLOG, and a Swedish flag. The main title is "14 NOV DATA PROTECTION OFFICERS PERSONALLY LIABLE FOR FINES". Below the title, it says "Posted at 16:20h in english, GDPR by admin". The text of the post discusses the personal liability of DPOs in Switzerland and the UK, mentioning that companies are seeking compensation from DPOs who acted wilfully or negligently. It quotes a statement: "...there are actions to take to avoid any liability...". The post further explains that while DPOs have clear duties, damages are directed against the controller or processor, not the DPO himself. It concludes by asking if a DPO can be personally liable for not performing his tasks.

В настоящее время вопрос личной ответственности DPO рассматривается в судах как в Швейцарии, так и в Великобритании. В обоих случаях компании, которые понесли расходы в рамках выплат административных штрафов за нарушение норм GDPR, требуют компенсацию от DPO, которые, по их утверждению, действовали преднамеренно или явно небрежно.

Личная ответственность DPO может возникнуть в случае, если он не выполнил свои обязанности по доведению информации о выявленных несоответствиях до руководства или обязанности по предоставлению активных рекомендаций по выполнению требований GDPR.

DPO не несет ответственности за определение приоритетов и выполнение действий, направленных на улучшение конфиденциальности и соблюдение GDPR. Эта ответственность ложится на контролера данных или процессора.

## Legal risks to being a DPO

Carlisa Hanvatty

iapp

Data protection officers may have tremendous job security under Article 38(3) of the European Union's General Data Protection Regulation, but the job may also come with hidden risks. In some countries, DPOs – or their equivalent under local law – may be held personally liable for failing to comply with local privacy law. For example, an employment agency's sole corporate director recently pleaded guilty to a criminal offense under Hong Kong's Personal Data Privacy Ordinance, specifically for failing to respond to a summons for investigation under section 50B(1)(b) of PDPO. Although criminal prosecutions under the law are not new, this case marked the first time it has occurred for the mere failure to respond to an investigation.

In fact, a number of data protection and privacy laws around the world expose DPOs to personal civil and criminal liability under a variety of circumstances. Prospective DPOs may want to ask their employers a number of questions, addressed below, regarding how best to mitigate the risk of personal responsibility.

### Personal liability provisions under data protection laws

#### 1. Canada

Canada's Anti-Spam Law (CASL) prohibits sending any "commercial electronic message" without the prior express or implied consent of the recipient. Fines are assessed by the Canada Radio Television Commission, which oversees and enforces CASL. However, a section of CASL provides for a private right of action allowing individuals and corporations to sue

alleged infringers of the law, although that section, which was due to come into force July 1, 2017, has been suspended pending parliamentary review.

Should this right come into force, it would mean that, in addition to potential statutory damages, courts will be able to order individuals held liable under CASL to pay the complainants an amount equal to their actual loss or damage. Under this law, companies' directors and officers can be found personally liable under certain provisions of CASL if they directed, authorized, assented to, acquiesced in or participated in the commission of a contravention of CASL.

#### 2. Hong Kong

Hong Kong's Personal Data (Privacy) Ordinance (PDPO), overseen by Hong Kong's Privacy Commissioner for Personal Data, allows civil or criminal proceedings against any "data user" (defined as "a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data"), for a variety of offenses, including failing to acquire consent before using data in direct marketing, providing personal data to a third party without consent, providing false information to the commissioner, even failing to comply with an enforcement notice. Further, section 66 provides for compensation to "an individual who suffers damage" (including "injury to feelings") from the data user for that damage. Data subjects can even apply to the commissioner for assistance in recovering that compensation. Maximum penalties for breaches under the PDPO are fines of up to HK\$1 million (approximately U.S. \$130,000) and imprisonment for up to

	Statute	Civil liability	Criminal liability	Penalty	Imprisonment
Canada	CASL (Section 31, currently suspended)	"[I]f directed, authorized, assented to, acquiesced in or participated in" violation of CASL	N/A	Statutory damages and compensation for actual loss or damage	N/A
Hong Kong	PDPO	"Subject to subsection (4), an individual who suffers damage by reason of a contravention— (a) of a requirement under this Ordinance; (b) by a data user; and (c) which relates, whether in whole or in part, to personal data of which that individual is the data subject, shall be entitled to compensation from that data user for that damage."	Data user: "a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data"  "[I]f the data is provided for gain, to a fine of \$1000000 and to imprisonment for 5 years"	Statutory damages and compensation for damage	Up to 5 years
Ireland	Data Protection (Amendment) ACT 2003 (Section 29)	N/A	"[C]ommitted with the consent or connivance of or to be attributable to any neglect on the part of a person"	Statutory Damages	N/A
Malaysia	PDPA (Part X, Section 133)	N/A	"[W]as in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management— (a) may be charged severally or jointly"	Statutory Damages	Up to 2 years
Philippines	DPA (Rule XIII, Section 61)	"[T]he penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime."	"[T]he penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime."	Statutory damages	6 months -7 years
Singapore	PDPA (Part X, 52 (1))	"Where an offence under this Act committed by a body corporate is proved (a) to have been committed with the consent or connivance of an officer, or (b) to be attributable to any neglect on his part..."	"[T]he officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly."	Statutory damages and private right of action	1-3 years
United Kingdom	DPA (Part VI Section 55A)	N/A	"(a) [K]new or ought to have known (i) that there was a risk that the contravention would occur, and (j) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but (b) failed to take reasonable steps to prevent the contravention."	Statutory Damages	N/A



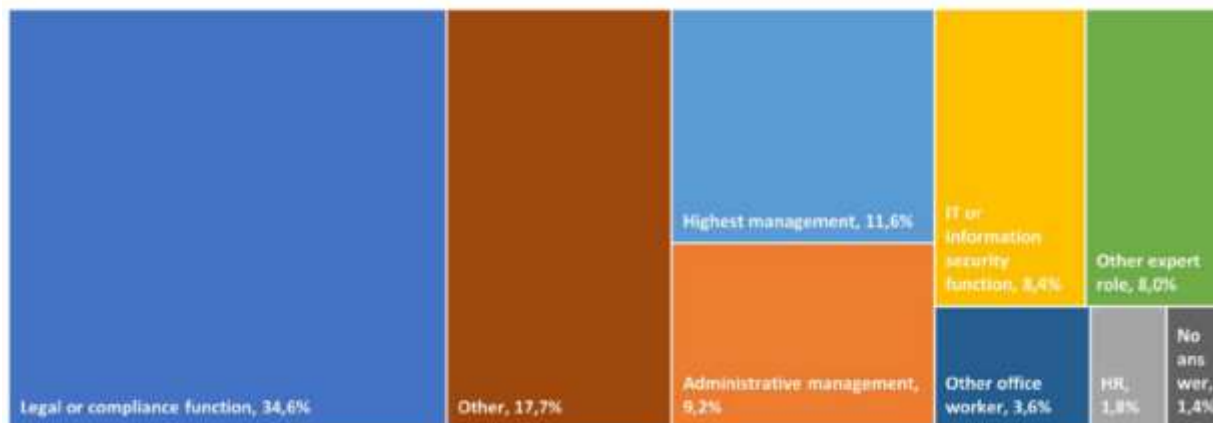
6 января 2020 года Сеульский восточный окружной суд признал Ким Джин-Хвана, DPO южнокорейского туристического агентства Hana Tour Service Inc., виновным в халатности из-за неспособности предотвратить утечку данных 2017 года, которая затронула 465,000 клиентов агентства и 29,000 работников Hana Tour.

DPO был обвинен в нарушении Закона о защите персональной информации и Закона о сетях, в соответствии с которыми DPO должен принимать необходимые «технологические и управленческие меры», чтобы предотвратить утечку данных, а также обязан уведомлять Комиссию по связи Кореи о любых случаях нарушения безопасности персональных данных в течение 24 часов.

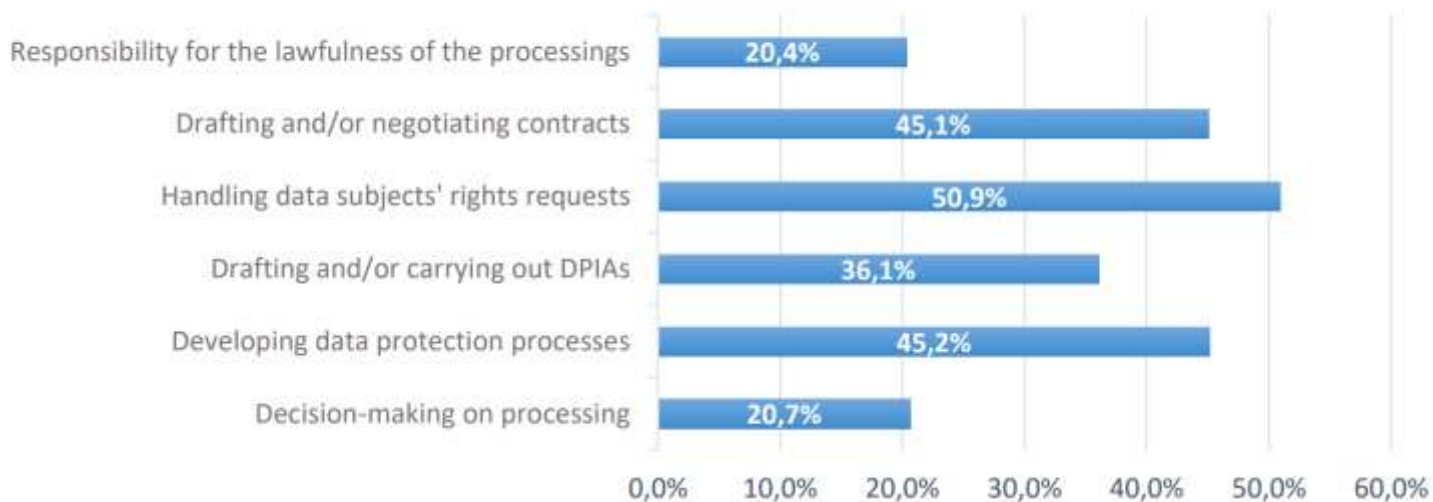
Суд наложил штраф в размере 10,000,000 южнокорейских вон (ок. \$8,500) на DPO в дополнение к штрафу в 327,250,000 вон (ок. \$280,000), ранее наложенному на агентство Министерством внутренних дел и безопасности Кореи.

## Отчет EDPB об областях улучшения для продвижения роли и признания DPO

### Q8: Where do DPOs work?

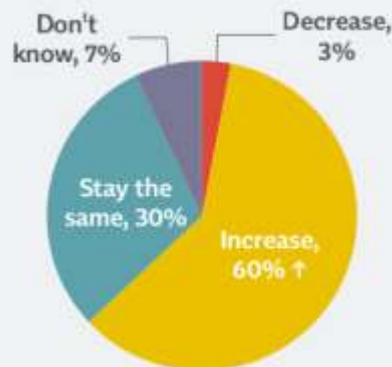


### Q17. Which of the following additional tasks are committed/assigned to the DPO?



## Отчет IAPP и EY за 2021 г. об управлении защитой персональных данных в компаниях

In next 12 months, privacy budget will...  
(Base: Director or higher)

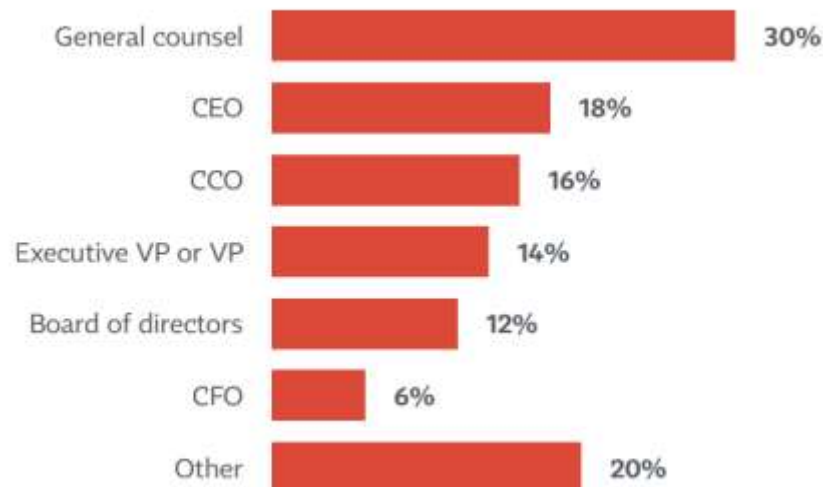


↑ Significantly different from 2020

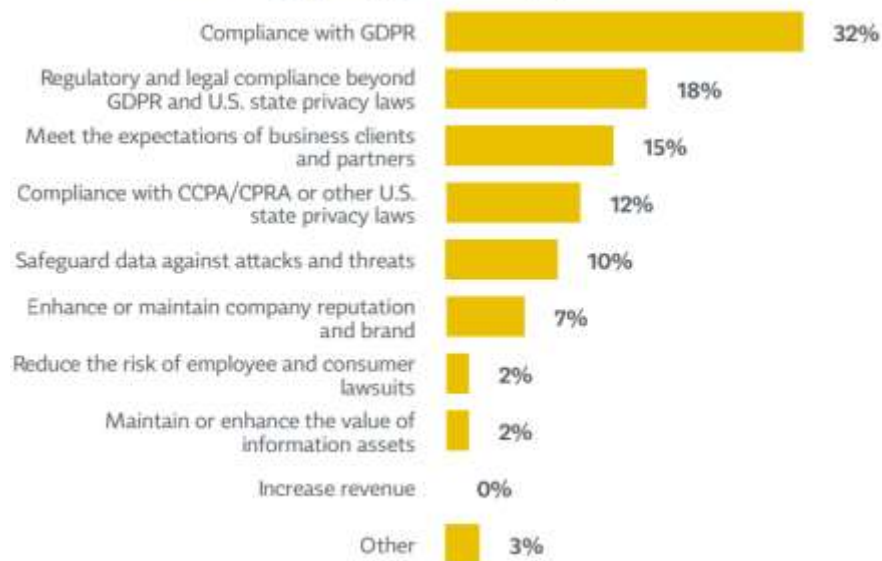
“Schrems II” decision  
(Adds to more than 100% because respondents could choose more than one)



### To whom privacy leader reports



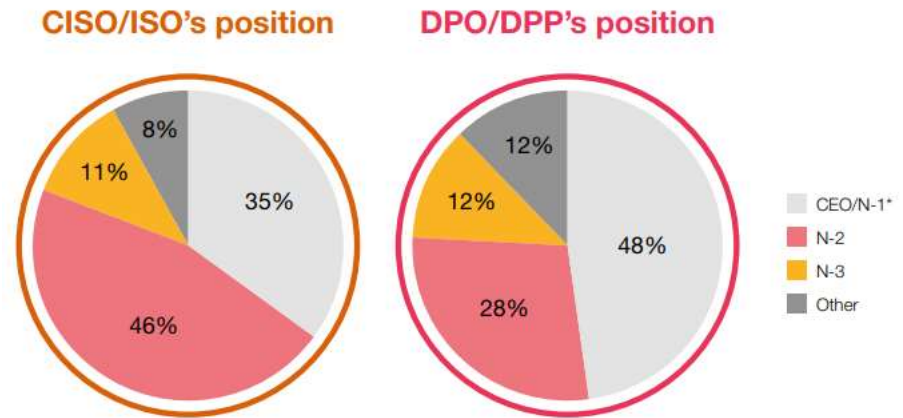
### Privacy program top priorities



## Education, Skills, Experience, Profiles & Positions



### The CISO/ISO's and DPO's position within the company



## CISOs' and DPOs' main challenges

### The CISO/ISO's and DPO's role (additional functions they occupy)

85% of CISOs' respondents are full-time in the CISO role.

68% of DPOs' respondents are full-time in the DPO role.

Among "part-time DPOs",

**87.5%** respondents allocate in most cases **25%** of their time to their DPO role.

The remaining **75%** of the time is allocated to their other roles.



#### CISO/ISO



Effectively dealing with threats and budget.



Improving the awareness of risks and the awareness of CISO role.



Effectively working with IT.

#### DPO/Data privacy professionals



Increasing the awareness on GDPR.



The application and enforcement of GDPR.

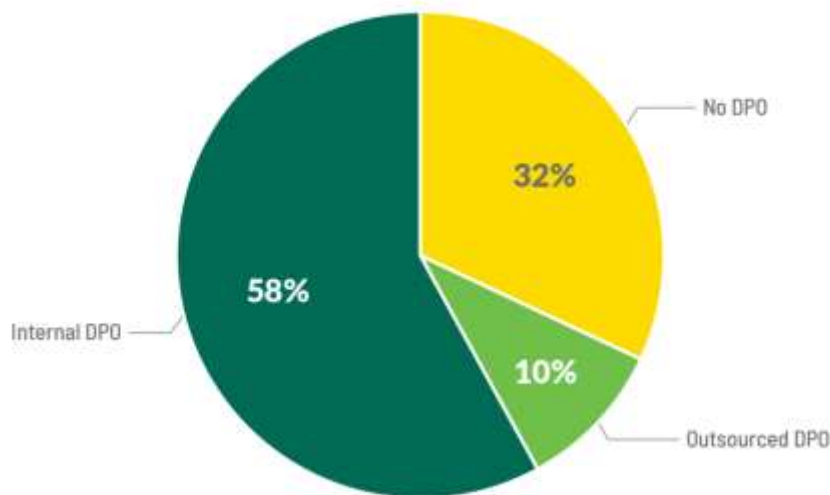


The involvement of the DPOs.

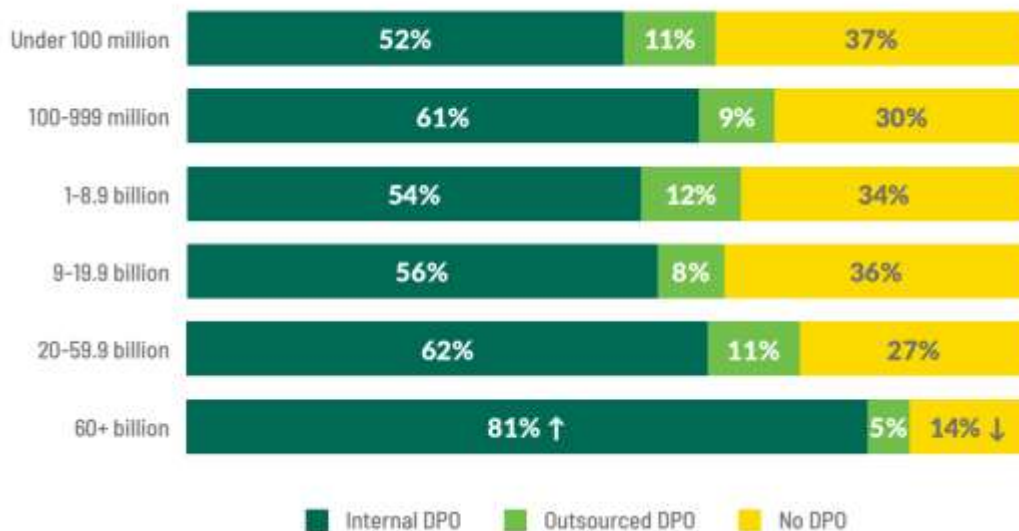
• 88% of DPOs declare having **no budget**.

# Отчет IAPP и EY за 2023 г. об управлении информационной приватностью в компаниях

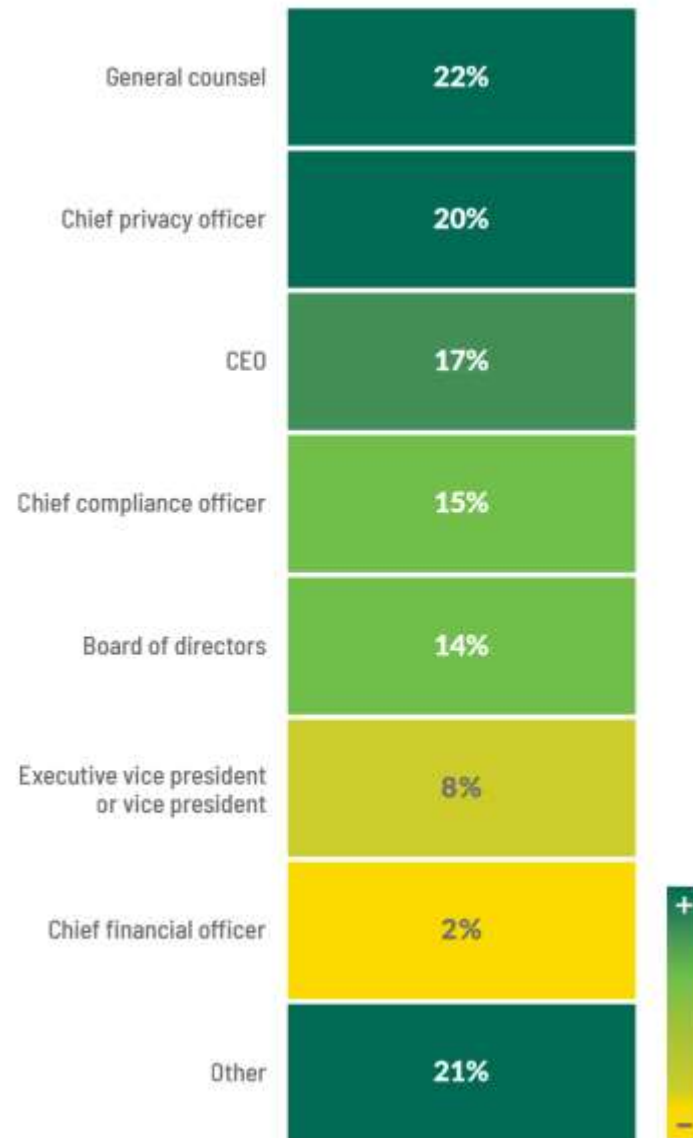
### Existence of DPO in an organization



### Existence of DPO by annual revenue in USD



### Who does the DPO report to?





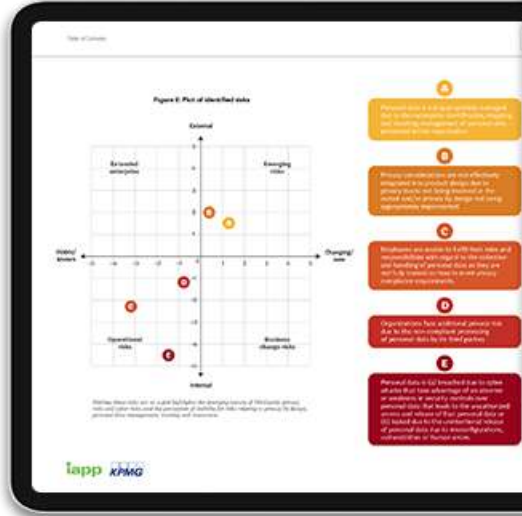
## КАКИЕ ЗАДАЧИ ВХОДЯТ КОМПЕТЕНЦИЮ СПЕЦИАЛИСТА ПО ЗАЩИТЕ ДАННЫХ (DPO)?



## ГДЕ ИСПОЛЬЗУЕТСЯ СПЕЦИАЛИЗИРОВАННОЕ ПО



# Отчет IAPP и KPMG за 2023 г. об управлении рисками информационной приватности в компаниях



- A** Privacy risks in AI that are not fully understood, including the potential for bias, discrimination, and data misuse.
- B** Privacy compliance gaps and risk, especially around data processing and data sharing, and the impact of new regulations.
- C** Hardware and software vulnerabilities, including the impact of the supply chain and the potential for data breaches.
- D** Organizations face additional privacy risk in AI that is not fully understood, including the potential for bias, discrimination, and data misuse.
- E** Personal data in AI is used to make decisions that have a significant impact on individuals, including the potential for bias, discrimination, and data misuse.

## 43% of organizational leaders think it is likely that in the next two years, a cyberattack will materially affect their own organization.

**Further exploring the**

Personal data in AI revealed due to cyberattacks that take advantage of an absence or weakness in security controls. Personal data that leads to the unauthorized access and release of that personal data is 10x more likely to be the organizational release of personal data due to unauthorized access or misuse.

As the 2023 Cyber Security Report, CyberRisk Intelligence by IBM Security, states: "The 2023 compared to the previous year, with an average of 1.5x more attacks per organization being reported." The 2023 Cyber Security Report also states: "The 2023 compared to the previous year, with an average of 1.5x more attacks per organization being reported." The 2023 Cyber Security Report also states: "The 2023 compared to the previous year, with an average of 1.5x more attacks per organization being reported."

### Key takeaways

- The five highest privacy risks identified by participants were data breach, data request, third party data processing, software privacy, and data governance, highlighting personal data management and security risks.
- Additional top ranked emerging risks included hardware and software vulnerabilities, data management and governance were the top three most common risks identified by participants.

**21%**

Only about 21% of organizations empowered the third line of defense to undertake privacy audits.

**30%**

Almost 30% of organizations use spreadsheet technology to help manage their privacy risk efforts.

**50%**

Only 50% of organizations have an established privacy risk appetite.

**64%**

64% of organizations have a privacy risk management program that is fully integrated into their overall enterprise risk management program.

**83%**

83% of organizations place some kind of privacy risk information in their annual report.

**93%**

Almost 93% of organizations indicated privacy is a top-10 organizational risk, and 36% ranked it within the top five.

**21%**

Only about 21% of organizations empowered the third line of defense to undertake privacy audits.

**30%**

Almost 30% of organizations use spreadsheet technology to help manage their privacy risk efforts.

**50%**

Only 50% of organizations have an established privacy risk appetite.

**64%**

64% of organizations have a privacy risk management program that is fully integrated into their overall enterprise risk management program.

**83%**

83% of organizations place some kind of privacy risk information in their annual report.

**93%**

Almost 93% of organizations indicated privacy is a top-10 organizational risk, and 36% ranked it within the top five.

## Profile of professionals by region

Department privacy leader is based	Total	U.S.	Canada	EU	U.K.	Other
Legal	49%	<b>58%</b>	<b>26%</b>	47%	42%	<b>38%</b>
Regulatory compliance	15%	13%	<b>23%</b>	14%	18%	14%
Information security	6%	8%	<b>1%</b>	6%	5%	8%
Information technology	6%	5%	<b>11%</b>	<b>3%</b>	6%	<b>14%</b>
Corporate ethics	4%	5%	<b>0%</b>	4%	4%	4%
Finance and accounting	2%	<b>1%</b>	5%	<b>5%</b>	2%	0%
Human resources	1%	1%	1%	1%	1%	1%
Government affairs	1%	1%	0%	2%	1%	1%
Internal audit	1%	1%	0%	1%	1%	0%
Records management	1%	0%	<b>4%</b>	0%	1%	0%
Public relations	0%	0%	<b>3%</b>	0%	0%	0%
Other	13%	<b>7%</b>	<b>26%</b>	17%	<b>19%</b>	20%

## Зарплаты профессионалов в сфере приватности – исследование IAPP 2021 года

### Privacy professionals' salaries (in USD \$000) by job title

Title	Median	Mean
Chief privacy officer	\$200.0	<b>\$212.3</b>
Lead privacy counsel	\$175.0	<b>\$177.5</b>
Director of privacy	\$160.0	<b>\$163.7</b>
Deputy chief privacy officer	\$164.0	\$161.2
Privacy engineer	\$148.0	\$146.6
Privacy counsel	\$135.0	\$140.7
Privacy officer	\$130.0	\$135.7
Data protection officer (non-mandated)	\$107.1	\$124.6
Data privacy manager	\$122.0	\$122.9
Data protection officer (GDPR mandated)	\$111.2	<b>\$117.0</b>
Privacy manager	\$104.0	<b>\$109.3</b>
Privacy analyst	\$80.3	<b>\$87.2</b>

### Average salary (in USD \$000) over time

Among all	2015	2017	2019	2021
Median	\$110.8	\$115.0	\$123.0	\$126.0
Mean	\$152.1	\$123.0	<b>\$134.3</b>	<b>\$140.5</b>

BASE SALARY IS LISTED WITHOUT PARENTHESES;  
TOTAL COMPENSATION IS INDICATED IN PARENTHESES.

	BIG TECH	FINANCIAL/ HEALTHCARE/ HEALTHCARE TECH	TELECOMM/ RETAIL/ ENTERTAINMENT
Entry Level	\$60K - 85K (\$70K - 95K)	\$60K - 85K (\$70K - 95K)	\$60K - 75K (\$70K - 85K)
Privacy Analyst/ Specialist	\$90K - 140K (\$90K - 165K)	\$90K - 140K (\$90K - 165K)	\$90K - 130K (\$90K - 150K)
Privacy Program/ Project Manager	\$140K - 180K (\$165K - 250K)	\$130K - 160K (\$145K - 175K)	\$130K - 160K (\$145K - 175K)
Privacy Sr. Manager/ Consultant	\$175K - 200K (\$200K - 250K)	\$140K - 170K (\$160K - 190K)	\$140K - 160K (\$160K - 180K)
Privacy Directors/ SMEs	\$225K - 300K (\$300K - 400K)	\$200K - 260K (\$230K - 320K)	\$200K - 250K (\$230K - 300K)
Privacy Engineer	\$175K - 300K (\$225K - 460K)	\$150K - 235K (\$175K - 360K)	\$150K - 205K (\$175K - 325K)
Privacy Counsel	\$225K - 325K (\$275K - 450K)	\$200K - 300K (\$250K - 400K)	\$175K - 320K (\$200K - 400K)
CPOs/ Business Unit Privacy Leads	\$265K - 465K (\$325K - 1.5MM)	\$235K - 425K (\$275K - 800K)	\$225K - 315K (\$275K - 600K)

All data reflected above is in USD and reflects US compensation ranges.  
TRU can consult on global geographic compensation adjustments upon request.

# Зарплаты профессионалов в сфере приватности – исследование IAPP и TRU 2023 года

## FINANCIAL COMPENSATION

OVERALL AVERAGE BASE SALARY

**\$146,200**

FOR INTERNAL PRIVACY PROFESSIONALS

↑ **7%** FROM 2021\*

↑ **10%** FROM 2019\*

\*When adjusted for sample distribution and currency exchanges.

HIGHEST INTERNAL AVERAGE BASE SALARY

**Global CPO**  
**\$206,000**

HIGHEST EXTERNAL AVERAGE BASE SALARY

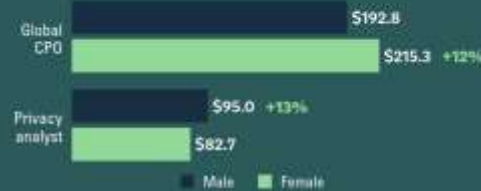
**Privacy LAWYER**  
**\$200,800**

## EXAMINING THE GENDER PAY GAP



Across all roles, female respondents earned 1% more on average in their base salaries than male respondents. Variation exists among specific roles, with female global chief privacy officers reporting 12% higher base salaries and male privacy analysts earning 13% more.

Average base salary (in \$000) by role by gender, with gender pay gap by role



Cash compensation in both base salary and bonus is still the primary means by which employers retain and attract talent.

IN THE PREVIOUS 12 MONTHS...



Nearly 8 in 10 of respondents received a raise.



Almost 7 in 10 of respondents received a bonus.

## LOCATION



U.S. privacy pros make 55% more on average in their base salaries compared to their European counterparts. This rises to 103% more depending on the specific role.



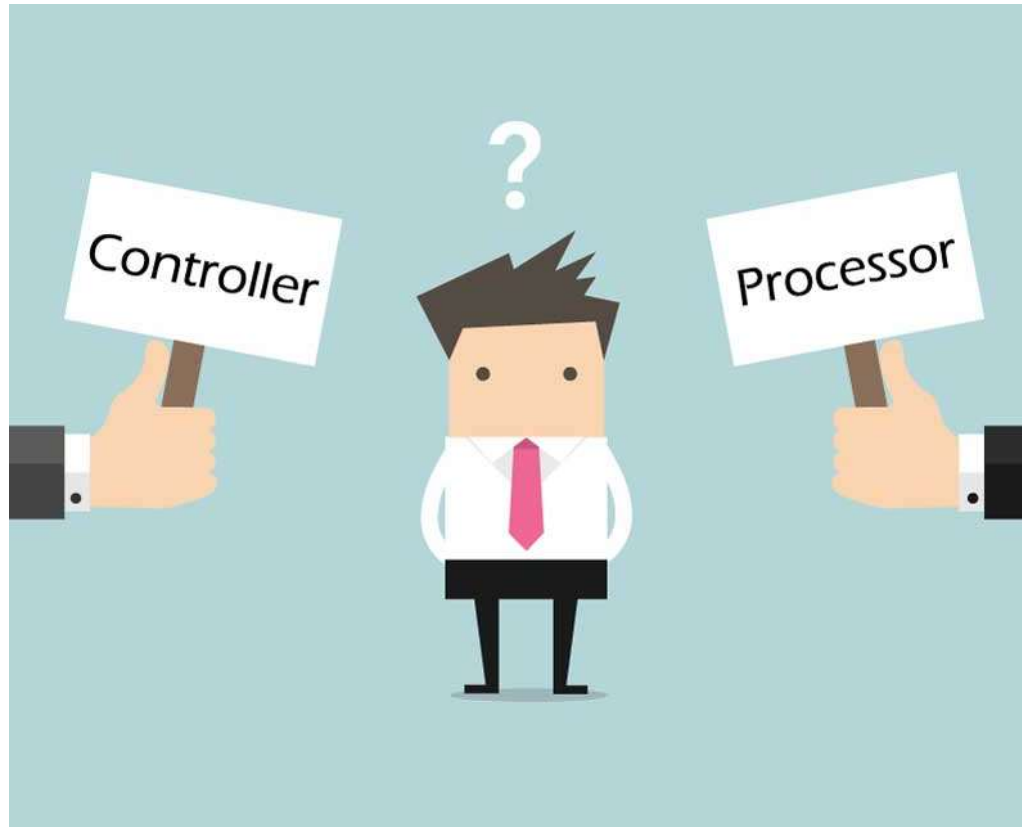
## JOB SATISFACTION

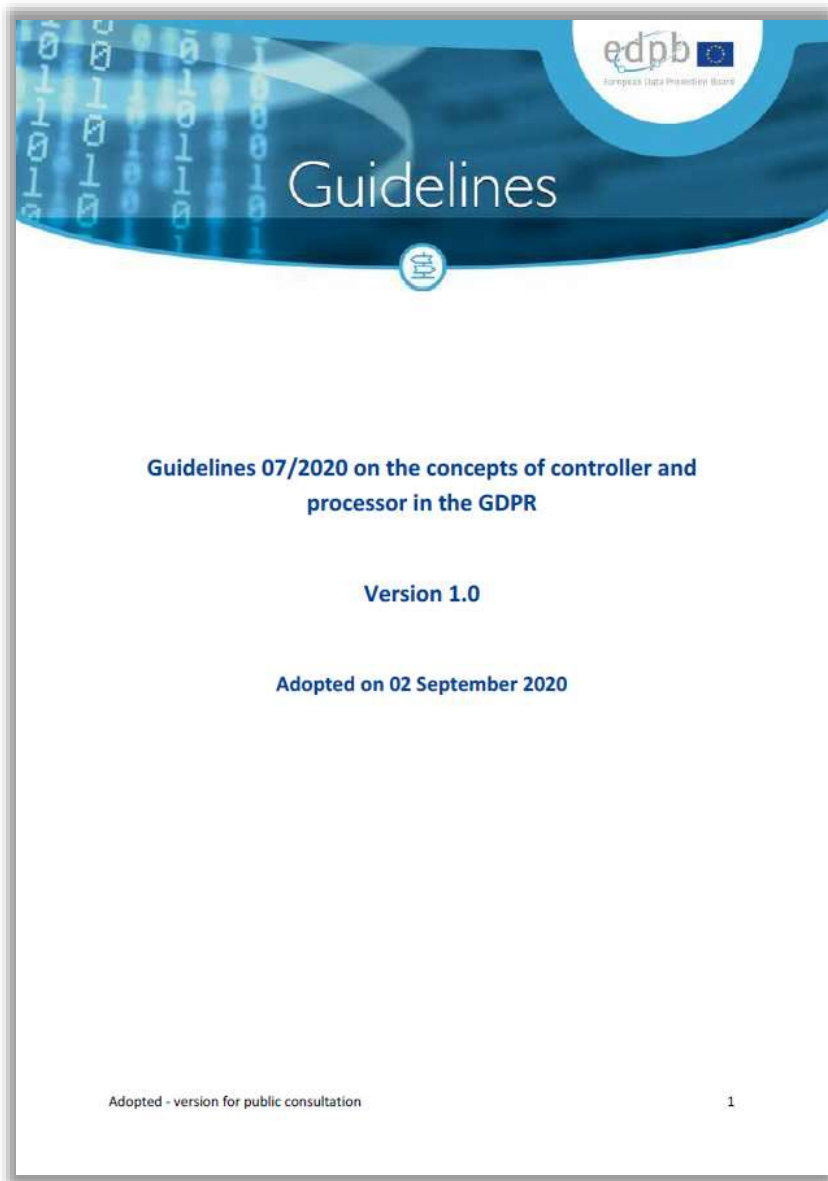
Job satisfaction of privacy pros, where 0 means not satisfied at all and 10 means extremely satisfied



Respondents were overwhelmingly satisfied with their current roles, with 86% reporting they were satisfied and 61% selecting a score above eight out of 10, where 10 is extremely satisfied.

## Роли в обработке персональных данных

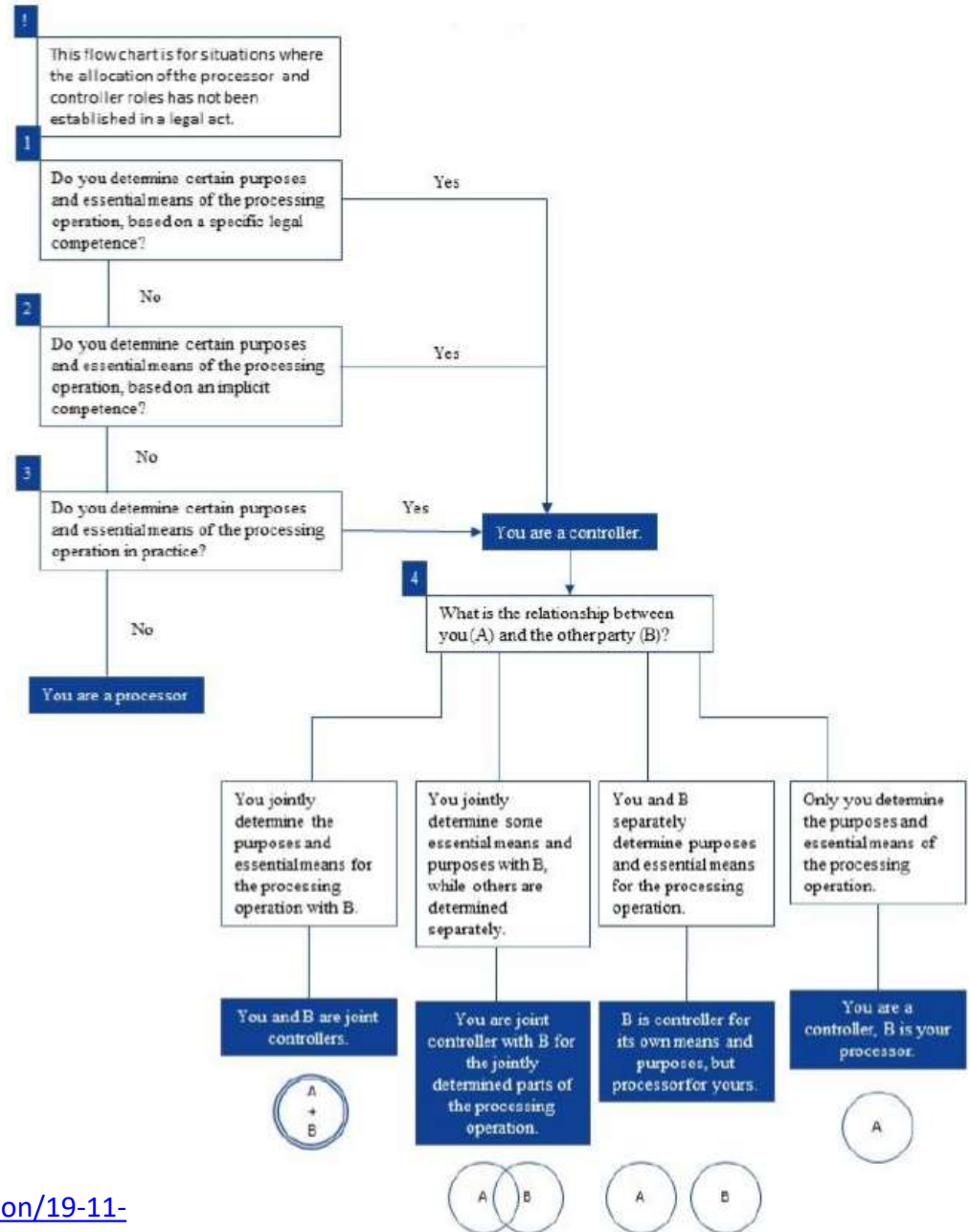
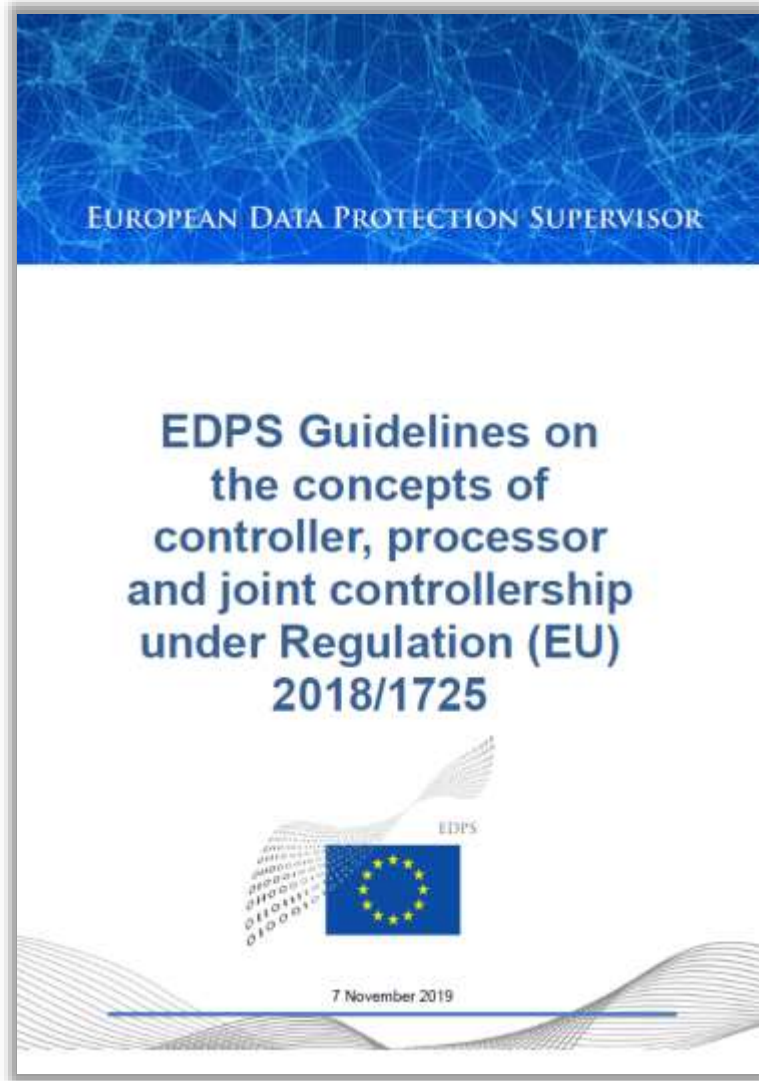




<b>PART I – CONCEPTS</b> .....	<b>8</b>
<b>1 GENERAL OBSERVATIONS</b> .....	<b>8</b>
<b>2 DEFINITION OF CONTROLLER</b> .....	<b>9</b>
2.1 Definition of controller .....	9
2.1.1 “Natural or legal person, public authority, agency or other body” .....	10
2.1.2 “Determines” .....	10
2.1.3 “Alone or jointly with others” .....	12
2.1.4 “Purposes and means” .....	13
2.1.5 “Of the processing of personal data” .....	15
<b>3 DEFINITION OF JOINT CONTROLLERS</b> .....	<b>16</b>
3.1 Definition of joint controllers .....	16
3.2 Existence of joint controllership .....	17
3.2.1 General considerations .....	17
3.2.2 Assessment of joint participation .....	18
<b>4 DEFINITION OF PROCESSOR</b> .....	<b>24</b>
<b>5 DEFINITION OF THIRD PARTY/RECIPIENT</b> .....	<b>27</b>
<b>PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES</b> .....	<b>29</b>
<b>1 RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR</b> .....	<b>29</b>
1.1 Choice of the processor .....	29
1.2 Form of the contract or other legal act .....	30
1.3 Content of the contract or other legal act .....	32
1.4 Instructions infringing data protection law .....	38
1.5 Processor determining purposes and means of processing .....	39
1.6 Sub-processors .....	39
<b>2 CONSEQUENCES OF JOINT CONTROLLERSHIP</b> .....	<b>40</b>
2.1 Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR .....	40
2.2 Allocation of responsibilities needs to be done by way of an arrangement .....	42
2.2.1 Form of the arrangement .....	42
2.2.2 Obligations towards data subjects .....	43
2.3 Obligations towards data protection authorities .....	45

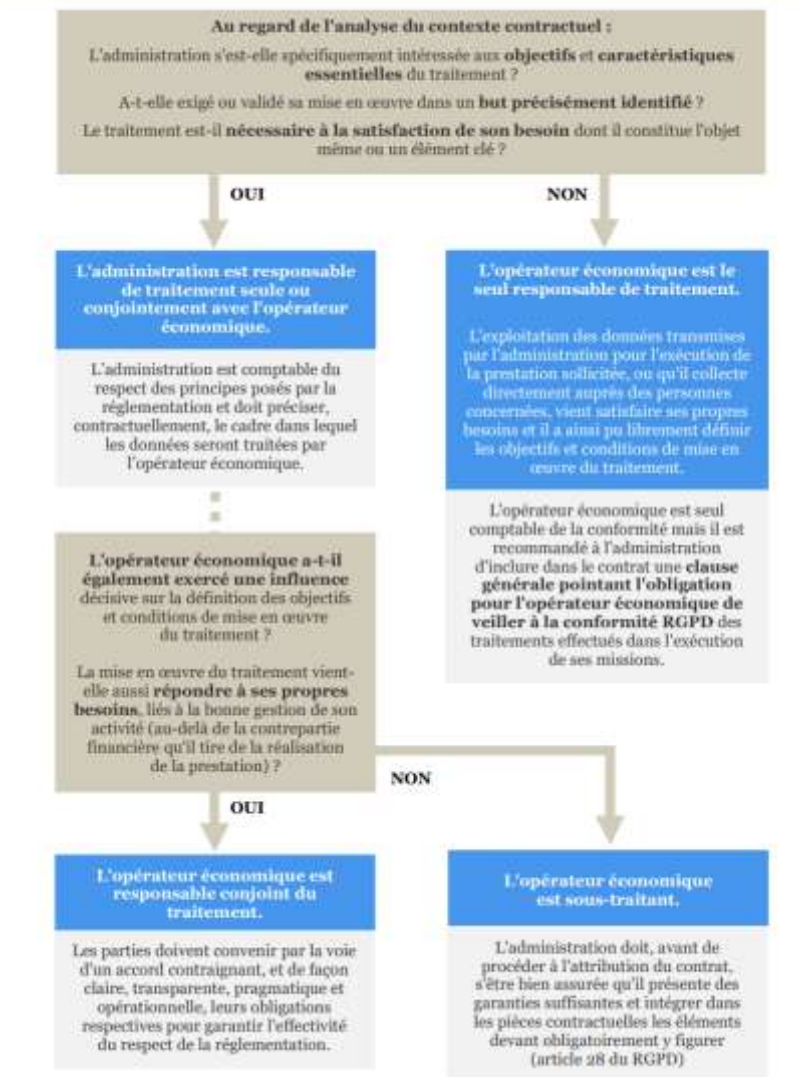


# Руководство EDPS по определению ролей controller, processor и joint controllers





## Schéma récapitulatif



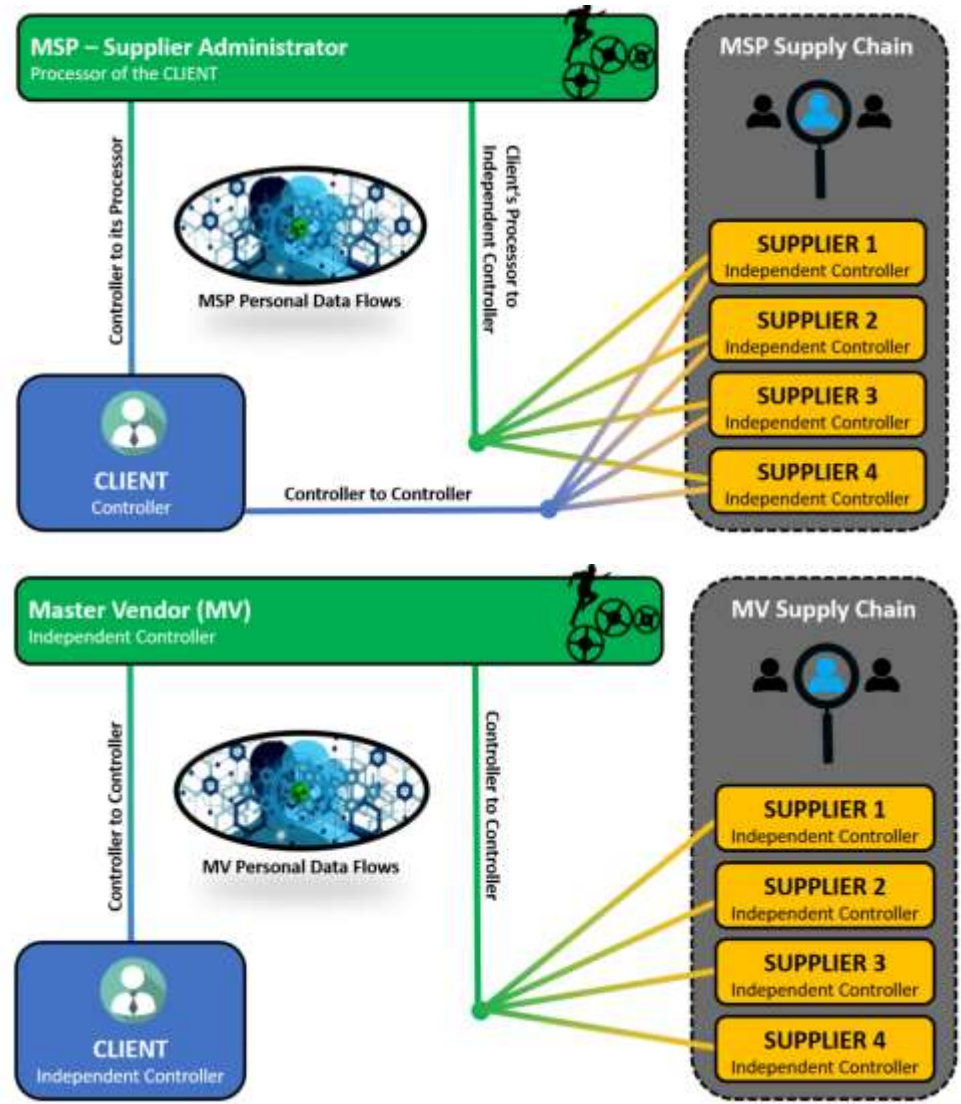
# Руководство WEC по определению роли в обработке данных для поставщиков кадровых услуг

**WORLD EMPLOYMENT CONFEDERATION**  
WEC Guidelines on Data Processing Roles for HR Service Providers:  
**CONTROLLER OR PROCESSOR?**

**Content:**

Disclaimer	Page 2
Introduction	Page 2
Data processing roles in relation to HR Services	Page 2
Controller or Processor	Page 3
o Data Controller	Page 3
o Data Processor	Page 4
o Purpose and Means of Processing	Page 4
The Three Data Processing Relationship Types	Page 5
o Controller-Controller	Page 5
o Controller-Processor	Page 6
o Joint Controller	Page 6
o Further Reading	Page 7
Applying the Data Privacy Roles to HR Services	Page 8
o Temporary Agency Work	Page 9
o Payrolling and Employment of Record	Page 11
o Direct Recruitment	Page 12
o Recruitment Process Outsourcing (RPO)	Page 13
o Outplacement/Career Management	Page 14
o Managed Service Provider (MSP)	Page 15
o Master Vendor (MV)	Page 17
About WEC Europe	Page 19

Task & Task Building - Avenue de l'Europe 102 - Box 102 - B-1050 Brussels - T + 32 2 231 18 01 - info@wecglobal.org - www.wecglobal.org Page 1/11



## Датский Datatilsynet разъяснил статус поставщиков услуг размещения серверов (colocation)

◇ Датский орган по защите информации (Datatilsynet) 03.10.2023 разъяснил, что поставщики услуг размещения серверов (colocation), как правило, не считаются обработчиками данных для своих клиентов, поскольку они предоставляют услуги, отличные от обработки персональных данных. Поставщики услуг colocation предоставляют только физическую инфраструктуру, включая Интернет и электропитание, и не имеют доступа к персональным данным, хранящимся на размещаемых ими серверах, особенно если клиенты используют свои собственные серверы и имеют эксклюзивный доступ к запертым серверным шкафам.

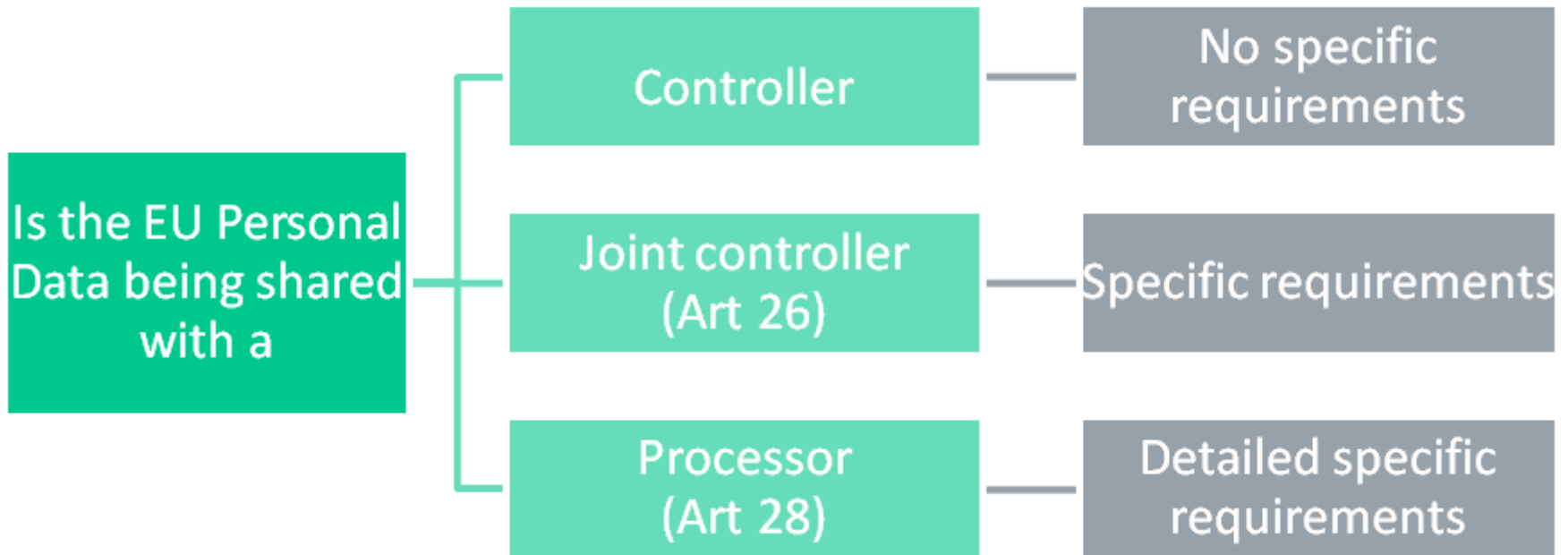
◇ Datatilsynet выделил следующие действия, которые могут определять провайдера услуг колокейшн как обработчика данных:

- доступ к персональным данным на серверах;
- замена или работа с аппаратными компонентами, такими как жесткие диски или память на размещенных серверах;
- управление, перезапуск или другие действия с серверами;
- предоставление дополнительных услуг, помимо физической инфраструктуры, например, обеспечение межсетевого экранирования, резервного копирования или других мер безопасности.

◇ Провайдеры colocation выступают в качестве контролеров данных при обработке персональных данных в целях обеспечения физической безопасности, в том числе при регистрации электронных брелоков или проведении видеонаблюдения.

◇ Компании, пользующиеся услугами colocation, обязаны как контролеры данных убедиться в том, что меры безопасности, применяемые провайдерами colocation, адекватно учитывают риски, связанные с конкретной деятельностью по обработке данных.

## Требования к взаимодействию между контролерами, процессорами и совместными контролерами

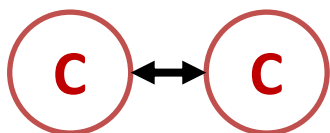


## Соглашения об обработке и защите персональных данных

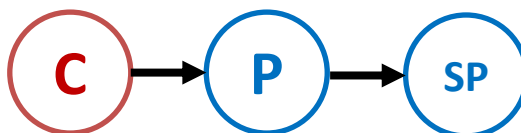


## Соглашение – универсальный инструмент регулирования обработки и защиты персональных данных в GDPR

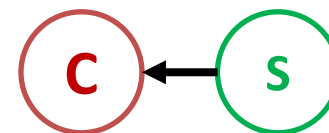
Существует большой потенциал такого универсального юридического инструмента как соглашение для урегулирования отношений об обработке и защите персональных данных между сторонами. Наиболее распространёнными и известными видами соглашений являются **DTA** и **DPA**. Стороной соглашения с контролером может быть и субъект данных. Такого рода отношения обычно не регулируются специальными соглашениями, но существует практика включения в соглашение с субъектом специального раздела о приватности – **SPA**.



**Data Transfer Agreement**  
(Controller-to-Controller)

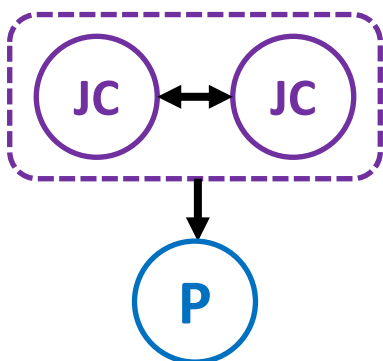


**Data Processing Agreement**  
(Controller-to-Processor/Subprocessor)

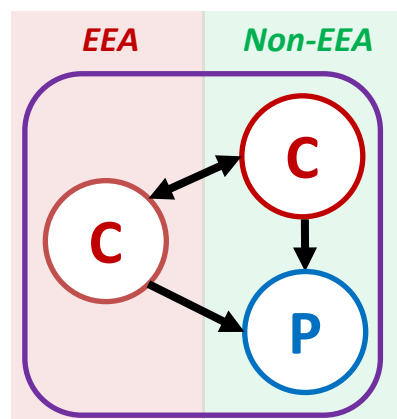


**Subject's Privacy Addendum**  
(Controller-to-Subject)

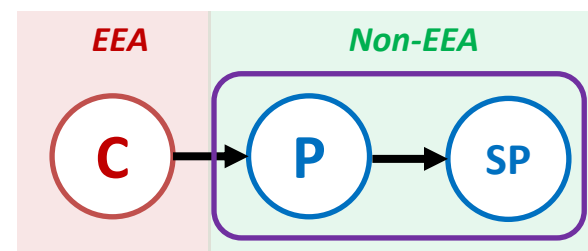
При этом GDPR фактически устанавливает режим большего разнообразия видов договорных отношений между участниками обработки персональных данных. Примером этого являются соглашения, направленные на структурирование сложных и часто трансграничных процессинговых активностей – **DMA** и механизм **BCR-C / BCR-P**.



**Data Management Agreement**  
(Joint Controllers)

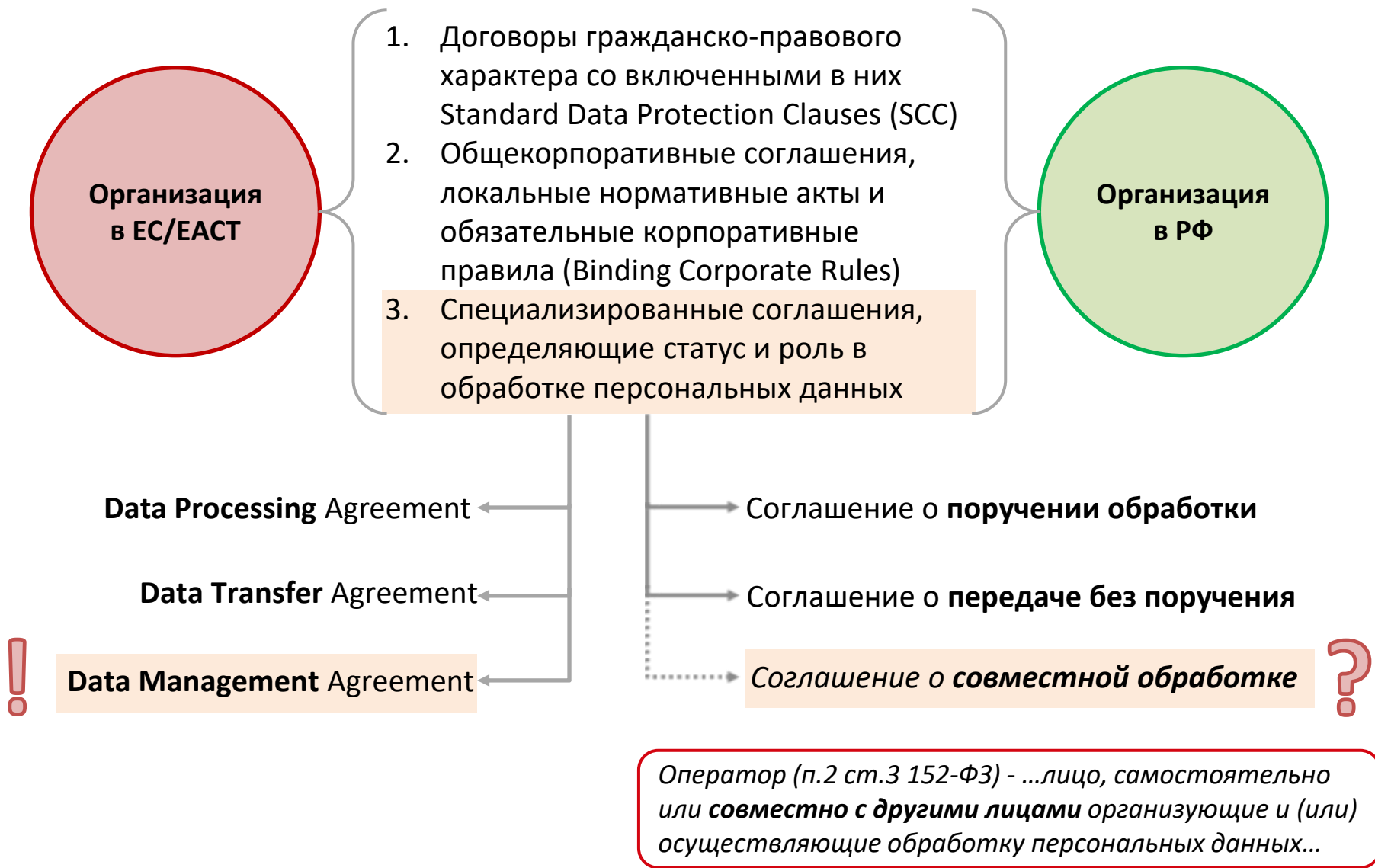


**Binding Corporate Rules – C**  
(Controller)



**Binding Corporate Rules – P**  
(Processor/Subprocessor)

## Механизмы договорного регулирования трансграничного оборота данных между организациями ЕС/ЕАСТ и РФ





**ico.**  
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters **For organisations** Make a complaint Action we've taken

For organisations / Data protection and Brexit /

## Controller to controller contract builder

Use this tool to build a contract when using standard contractual clauses to transfer personal data from an EEA-based controller to your UK-based organisation, as part of your preparations if the UK exits the EU without a deal.

Once you click start you will be asked a number of questions about the nature of the data you're transferring, the organisations. You will also be asked to tick any optional commercial clauses you would like to include.

A draft contract will be created. It will contain all the clauses you need, plus the information you provide about the data transfer and the additional clauses you select.

Download the draft contract as a word document. You will need to and complete the remaining specific details.

You will need to add in the details of the parties to the contract, which are marked for you to check and complete. You may also add more details where you have selected 'other' when answering any of the questions in the tool.

Both parties will need to sign the document before it is in force and valid.

Before signing you should consider seeking your own legal advice.

**Start now** →

All parties may wish to download this blank template of the contract, which contains guidance notes.

### Further reading

[Template contract with guidance](#)  
External link

**ico.**  
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters **For organisations** Make a complaint Action we've taken

For organisations / Data protection and Brexit / Controller to controller contract builder /

## Controller to controller contract builder

An asterisk (\*) indicates a required field.

### Step one of three: Fill in details about the personal data you are transferring

#### Q1. Who is the personal data about?

Please tick all that apply. \*

- Staff including volunteers, agents, temporary and casual workers
- Customers and clients (including their staff)
- Suppliers (including their staff)
- Members or supporters
- Shareholders
- Relatives, guardians and associates of the data subject
- Complainants, correspondents and enquirers
- Experts and witnesses
- Advisers, consultants and other professional experts
- Patients
- Students and pupils
- Offenders and suspected offenders

## DTA: Data Transfer Agreement как базовый способ построения отношений между контролерами

Data Transfer Agreement dated \_\_\_\_\_, 20\_\_

[Name of the counterparty], [address], established and operating in accordance with legislation of [name of the state], represented by [job title and full name of the authorized person], acting under [the basis of authority], on the one hand, and [Name of the counterparty], [address], established and operating in accordance with legislation of the Russian Federation, represented by [job title and full name of the authorized person], acting under [the basis of authority], on the other hand, hereinafter jointly referred to as the "Parties", and separately – as the "Party" (each Party may act in the capacity of both Party transferring personal data and the Party receiving personal data), have agreed on the following:

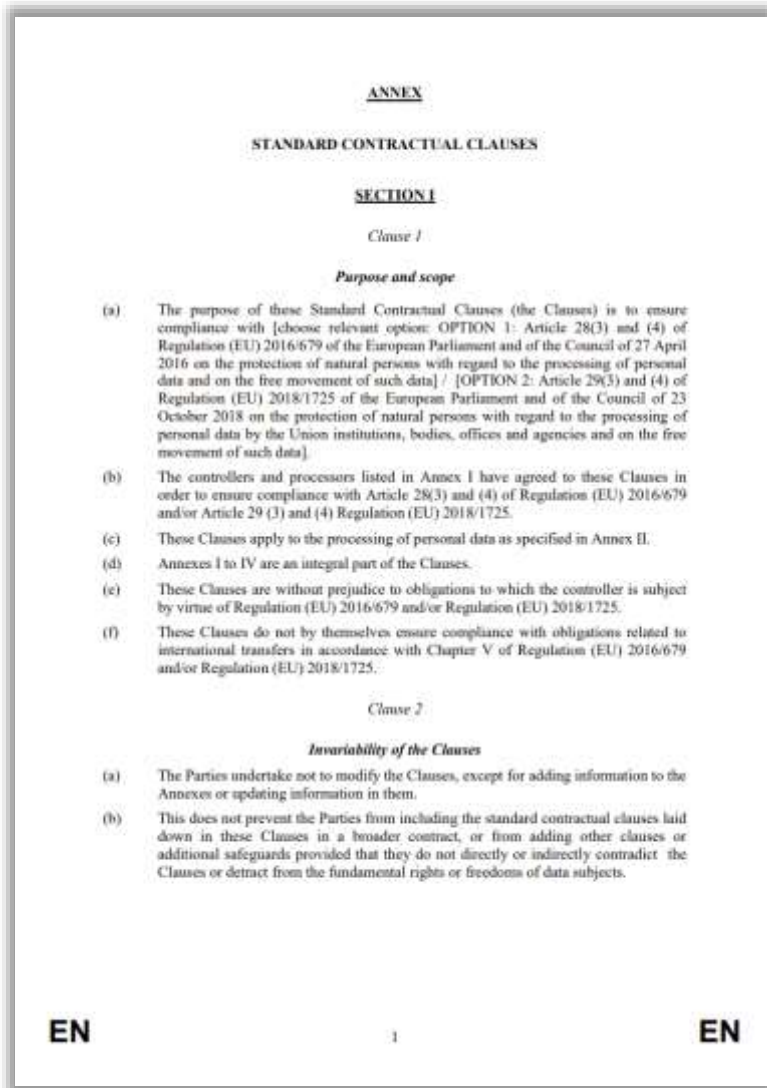
1. For the purpose of this Data Transfer Agreement including its exhibits (together, the "Agreement") the Parties apply the following terms and definitions:
  - (1) *personal data* means any information relating to a directly or indirectly identified or identifiable natural person (personal data subject or data subjects);
  - (2) *controller* means a legal entity arranging (alone or jointly with others) and (or) carrying out personal data processing, as well as defining the purposes of processing, the operations performed on the personal data (types of processing) and the categories of personal data that shall be processed;
  - (3) *transfer of personal data* means any act of sending and transmitting personal data by any means (including physical and electronic ones), providing access to personal data, including remote access and saving, inserting personal data in the information system(s);
  - (4) *reasonable time* means period of the time that a Party needs to fulfil an obligation under this Agreement determined jointly by the Parties on a case-by-case basis considering peculiarities of cooperation/interaction between the Parties, volume of the data transferred by the Parties, technical, organizational and other resources of the respective Party. In cases where compliance with statutory obligations implying mandatory terms/deadlines depends on fulfilment of obligations under this Agreement the determined reasonable time shall enable Parties to comply with the said statutory obligations.
2. The Parties warrant and guarantee transfer of personal data to each other on a lawful basis in accordance with requirements of applicable legislation and due notification of data subjects of such transfer if required by applicable legislation in order to achieve one, several or all of the purposes set out below that are relevant for the relationship between the Parties:
  - (1) concluding, performing and (or) terminating of contracts and agreements between the Parties;
  - (2) building and maintaining business relations between the Parties;
  - (3) carrying out due diligence procedures by the Parties;
  - (4) participating of one Party in the procurement procedures of the other Party;
  - (5) facilitating information interaction/communication between the Parties;
  - (6) exercising rights, fulfilling obligations and complying with prohibitions/restrictions under applicable rules.
3. Each Party acknowledges that it acts in the capacity of an independent controller of personal data received from the transferring Party (which acts as an independent controller as well) and that it, in common (but not jointly) with the other Party, determines the purposes and manner of personal data transfer between the Parties unless otherwise is specified in the agreement on the assignment of personal data processing (instruction on data processing) or in the agreement on joint controllership that may be concluded by the Parties in respect of certain personal data processing activities.
4. The receiving Party undertakes to cease processing of personal data (or ensure that such processing is ceased) received from the transferring Party, upon achievement of the purposes specified in this Agreement or where such purposes are no longer relevant as well as in case of failure to ensure the lawful basis of the personal data processing unless otherwise is specified in applicable legislation.
5. The Parties warrant and guarantee preserve confidentiality and security of the transferred personal data in the course of their processing in accordance with requirements of the applicable laws, as well as agreements between the Parties. The Parties shall take legal, organizational and technical measures that are necessary to protect personal data in the course of their transfer between the Parties via electronic communication channels, computer-readable and paper media or otherwise (or ensure that such measures are taken), if warranties or guarantees specified in this paragraph are inaccurate then the receiving Party shall immediately refuse to receive personal data from the transferring Party and (or) shall within a reasonable time stop processing personal data received from the transferring Party prior to that.
6. The transferring Party shall, within a reasonable time as of receipt of the relevant request from the receiving Party, provide the receiving Party with information and (or) documents confirming that it obtained consents of data subjects to transfer of their personal data, or that it relies on other legal grounds for the personal data transfer and it duly notified the subjects of the transfer of their personal data.
7. For the purposes specified in this Agreement, the receiving Party has the right to engage third parties to the processing of personal data received from the transferring Party by instructing third parties to process these personal data and (or) by transferring (including cross-border transfer) personal data to third parties without assigning of personal data processing (without giving instruction to process personal data on its own behalf). The engagement of third parties to the processing of personal data can be carried out only if receiving Party ensured appropriate legal grounds and only if the third parties undertake to preserve confidentiality and security of personal data in the course

- ✓ определяет статус сторон как самостоятельных контролеров в отношении получаемых персональных данных;
- ✓ фиксирует требования об осуществлении передачи персональных данных субъектов на законном основании, о надлежащем уведомлении субъектов при передаче их персональных данных и об обеспечении конфиденциальности и безопасности обработки полученных персональных данных;
- ✓ закрепляет принцип равноправия сторон при взаимной передаче персональных данных, не дает каких-либо преимуществ и не ущемляет интересы обеих сторон;
- ✓ является рамочным и бессрочным, то есть требует всего лишь однократного подписания и регулирует все договорные отношения между сторонами;
- ✓ защищает права и законные интересы субъектов при передаче их персональных данных;
- ✓ позволяет сторонам привлекать третьих лиц к обработке полученных персональных данных;
- ✓ снижает риск предъявления претензий к сторонам от надзорных органов в отношении соблюдения сторонами должной осмотрительности при осуществлении взаимной передачи персональных данных.

Подготовленный автором презентации проект DTA:

<http://sps-ib.ru/dta-eu.docx>


## Standard Contractual Clauses для взаимоотношений между контролером и процессором в ЕЭЗ



04.06.2021 Европейская Комиссия опубликовала новые Стандартные договорные условия для урегулирования отношений типа Controller-to-Processor на территории ЕЭЗ согласно ст.28(7) GDPR и ст.29(7) Регламента ЕС 2018/1725. Текст новых SCC был подготовлен с учетом позиции EDPB и EDPS.

SCC могут являться частью договорных отношений между контролером и процессором, но должны иметь преимущество перед ними с т.з. защиты прав и свобод субъектов.

## DPA: Первые национальные SCC Controller-to-Processor, утвержденные EDPB в декабре 2019 года




European Data Protection Board

☰ MENU

European Data Protection Board >

News > **EDPB News** > First standard contractual clauses for contracts between controllers and processors (art. 28 GDPR) at the initiative of DK SA published in EDPB register

### First standard contractual clauses for contracts between controllers and processors (art. 28 GDPR) at the initiative of DK SA published in EDPB register



🕒 Wednesday, 11 December, 2019 EDPB

Following the [EDPB opinion \(July 2019\) on the draft standard contractual clauses \(SCCs\)](#) for contracts between controller and processor submitted to the Board by the Danish Supervisory Authority (SA), the final text of the Danish SCCs, as adopted by the Danish SA, has been published in the EDPB's [Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism](#).

The standard processor agreement has been adopted by the Danish SA pursuant to art. 28(8) GDPR and aims at helping organisations to meet the requirements of art. 28 (3) and (4), given the fact that the contract between controller and processor cannot just restate the provisions of the GDPR but should further specify them, e.g. with regard to the assistance provided by the processor to the controller.

The possibility of using SCCs adopted by a SA does not prevent the parties from adding other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the adopted clauses or prejudice the fundamental rights or freedoms of the data subjects.

Nevertheless, the clauses are an instrument to be used "as is", i.e. the parties who enter into a contract with a modified version of the clauses are not deemed to have employed the adopted SCCs. On the contrary, to the extent that organizations choose to make use of these standard provisions, the Danish SA, for example in connection with an inspection visit, will not examine these provisions in more detail.

### 1. Table of Contents

2. Preamble .....	
3. The rights and obligations of the data controller .....	
4. The data processor acts according to instructions.....	
5. Confidentiality .....	
6. Security of processing .....	
7. Use of sub-processors .....	
8. Transfer of data to third countries or international organisations.	
9. Assistance to the data controller.....	
10. Notification of personal data breach.....	
11. Erasure and return of data.....	
12. Audit and inspection .....	
13. The parties' agreement on other terms .....	
14. Commencement and termination.....	
15. Data controller and data processor contacts/contact points .....	
Appendix A	Information about the processing .....
Appendix B	Authorised sub-processors .....
Appendix C	Instruction pertaining to the use of personal data...
Appendix D	The parties' terms of agreement on other subjects

**ico.**  
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters **For organisations** Make a complaint Action we've taken

For organisations / Data protection and Brexit /

## Controller to processor contract builder

Use this tool to build a contract when using standard contractual clauses to transfer personal data from an EEA controller to your UK-based organisation which is acting as a processor, as part of your preparations if the UK exits the EU without a deal..

Once you click start you will be asked a number of questions about the nature of the data you're transferring, the organisations involved and your security measures. You will also be asked to tick any optional clauses you would like to include.

A draft contract will be created. It will contain all the clauses you need plus the information you provide about the data transferred and any additional commercial clauses you selected.

Download the draft as a word document. You will need to add in details of the parties to the contract. You may also need to add further details about the security measures you use to protect the personal data.

Both parties will need to sign the document before it is in force and valid.

Before signing you should consider seeking your own legal advice.

**Start now** → ↗

Either party may wish to download the blank template of the contract, which contains guidance notes.

### Further reading

[Template with guidance notes](#)  
External link

The contract (or other legal act) sets out details of the processing including:

- the subject matter of the processing;
- the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data involved;
- the categories of data subject;
- the controller's obligations and rights.

The contract or other legal act includes terms or clauses stating that:

- the processor must only act on the controller's documented instructions, unless required by law to act without such instructions;
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract;
- the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights;
- taking into account the nature of processing and the information available, the processor must assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage; and
- the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations.

# General Data Protection Regulation

GUIDE FOR PROCESSORS  
SEPTEMBER 2017 EDITION

*Applicable from 25 May 2018 across the whole of the European Union, the General Data Protection Regulation (GDPR) strengthens European residents' rights bearing on their data and increases accountability on the part of all stakeholders processing such data (controllers and processors), whether or not they are established in the European Union.*

*The Regulation lays down specific obligations that must be followed by processors, who are likely to be held liable in the event of a breach.*

*This guide sets out to assist processors in implementing these new obligations.*

*All of the good practices reported by professionals may be added to it in time.*

## Example of sub-contracting contractual clauses

*The example of sub-contracting clauses below is provided pending the adoption of standard contractual clauses in the meaning of Article 28.8 of the GDPR. These examples of clauses can be inserted into your contracts. They must be tailored and specified according to the sub-contracting service concerned. Please note that they do not constitute a subcontract in themselves.*

[...], located in [...] and represented by [...]

(hereinafter, "**the controller**")

of the one part,

AND

[...], located in [...] and represented by [...]

(hereinafter, "**the processor**")

of the other part,

### I. Purpose

The purpose of these clauses is to define the conditions in which the processor undertakes to carry out, on the controller's behalf, the personal data processing operations defined below.

As part of their contractual relations, the parties shall undertake to comply with the applicable regulations on personal data processing and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which is applicable from 25 May 2018 (hereinafter "**the General Data Protection Regulation**").

### II. Description of the processing being subcontracted out

The processor is authorised to process, on behalf of the controller, the necessary personal data for providing the following service(s) [...].

The nature of operations carried out on the data is [...].

The purpose(s) of the processing is(are) [...].

The personal data processed are [...].

The categories of data subjects are [...].

To perform the service covered herein, the controller shall provide the processor with the following necessary information [...].

### III. Duration of the contract

This contract enters into force on [...] for a duration of [...].

### IV. Processor's obligations with respect to the controller

The processor shall undertake to:

1. process the data **solely for the purpose(s)** subject to the sub-contracting
2. process the data **in accordance with the documented instructions** from the controller appended hereto. Where the processor considers that an instruction infringes the General

## A Practical Guide to Controller-Processor Contracts



An Coimisiún um  
Chosaint Sonraí  
Data Protection  
Commission

The General Data Protection Regulation (GDPR), which came into force on 25 May 2018, introduced increased obligations for both data controllers ('controllers') and data processors ('processors'). One such obligation is the obligation on Controllers and Processors to enter into a legally binding contract governing the processing of personal data when a Processor is engaged to process personal data on the instruction of a Controller (a 'data processing contract').

This guidance note outlines in brief the context of the obligation on controllers and processors to enter into a data processing contract under the GDPR, when they need to enter into a data processing contract, and the minimum provisions which should be included in such a contract.

### Who needs to enter into Data Processing Contracts?

All controllers who engage processors to process personal data on their behalf are obliged to enter into a data processing contract. This obligation is relevant to controllers and processors in both the public and private sectors.

### Overview of Mandatory Provisions of Data Processing Contracts

Article 28(3) GDPR prescribes the provisions which must be included in a data processing contract between a controller and a processor. A controller and processor should enter into a data processing contract which must, at a minimum, contain the following details:

- The subject matter, duration, nature and purpose of the data processing;
- The type of personal data being processed;
- The categories of data subjects whose personal data is being processed; and
- The obligations and rights of the controller.

A data processing contract should also contain the following mandatory provisions:

- ✓ That the processor will only process personal data received from the controller on documented instructions of the controller (unless required by law to process personal data without such instructions) including in respect of international data transfers;
- ✓ That the processor ensures that any person(s) processing personal data is subject to a duty of confidentiality;

## A Practical Guide to Controller-Processor Contracts



An Coimisiún um  
Chosaint Sonraí  
Data Protection  
Commission

- ✓ That the processor takes all measures required pursuant to Article 32 GDPR (Security of Processing) including but not limited to implementing appropriate technical and organisational measures to protect personal data received from the controller;
- ✓ That the processor obtains either a prior specific authorisation or general written authorisation for any sub-processors the processor may engage to process the personal data received from the controller. The processor must further ensure that where a general written authorisation to the processor engaging sub-processors is obtained, the controller has the opportunity to object in advance to each individual sub-processor to be appointed by the processor;
- ✓ That any sub-processors engaged by the processor are subject to the same data protection obligations as the processor and that the processor remains directly liable to the controller for the performance of a sub-processor's data protection obligations;
- ✓ That the processor assists the controller by appropriate technical and organisational measures to respond to data subject rights' requests under the GDPR;
- ✓ That the processor assists the controller to ensure compliance with obligations under the GDPR in relation to security of data processing (Article 32 GDPR), notification of data breaches (Articles 33 and 34 GDPR) and data protection impact assessments (Article 35 and 36 GDPR);
- ✓ That, at the end of the data processing by the processor and on the controller's instruction, the processor deletes or returns the personal data received from the controller; and
- ✓ That the processor makes available to the controller all information necessary to demonstrate compliance with Article 28 GDPR and that the processor allows for and contributes to audits conducted by the controller or a third party on the controller's behalf.

### Other Provisions which May Be Included in Data Processing Contracts

There are a number of other provisions which controllers and processors may wish to include in data processing contract which are not mandatory for inclusion under the GDPR. Such provisions may include but are not limited to:

- Liability provisions (including indemnities);
- Detailed (technical) security provisions; and/or
- Additional cooperation provisions between the controller and processor.

## 272 DPA: Кодекс поведения для процессоров от LfDI Баден-Вюртемберг

Орган по защите данных Баден-Вюртемберга ("LfDI Baden-Württemberg") 18.11.2022 одобрил национальный кодекс поведения под названием "Требования к процессорам в соответствии со статьей 28 GDPR - Доверенный процессор данных", выпущенного Ассоциацией по продвижению кодексов поведения ("VFV") 09.06.2022. Кодекс поведения обеспечивает ясность и правовую определенность для компаний при обработке персональных данных в соответствии с GDPR.

Кодекс предназначен для процессоров во всех секторах, которые предлагают свои услуги на немецком рынке и обрабатывают персональные данные в Германии, по смыслу раздела 2 Руководства 1/2019 Европейского совета по защите данных ("EDPB") о кодексах поведения и органах мониторинга в соответствии с Регламентом 2016/679, принятого 4 июня 2019 года.

В дополнение к функциям мониторинга надзорного органа, кодекс поведения охватывает требования, среди прочего, в отношении:

- заключению договоров с субпроцессорами;
- права субъектов данных;
- информирование о нарушениях данных; и
- обязательства по соблюдению конфиденциальности.

Отныне компании могут добровольно принять на себя обязательства по соблюдению Кодекса под контролем контролирующего органа, который следит за соблюдением ими Кодекса и служит контактным лицом для подачи жалоб. С этой целью LfDI Баден-Вюртемберг заявил, что после утверждения кодекса поведения он аккредитовал Аккредитационное общество по защите данных ("DSZ") в качестве нового контролирующего органа для обработки заявок на получение статуса доверенного обработчика данных и мониторинга жалоб.



## **DPA: Руководство Lfd Niedersachsen Нижней Саксонии по заключению договоров с Microsoft 365**

Надзорный орган по защите данных Нижней Саксонии (LfD Niedersachsen) совместно с шестью другими немецкими надзорными органами по защите данных разработало и 22.09.2023 опубликовало руководство по работе со стандартным соглашением Microsoft об обработке заказов, известным как Дополнение о защите данных продуктов и услуг (Дополнение), при использовании Microsoft 365.

В руководстве указано, что в ноябре 2022 года Немецкая конференция по защите данных (DSK) опубликовала оценку Microsoft 365, в которой DSK определила, что Дополнение не соответствует требованиям ст.28(3) GDPR, и что данное руководство было разработано в связи с проблемами, отмеченными DSK. В частности, руководство предназначено для лиц, ответственных за заключение Дополнительного соглашения, с целью оказания им поддержки в работе над соответствующими изменениями в договоре.

Руководство включает:

- информацию об определении типа и цели обработки, а также типа персональных данных;
- ответственность Microsoft в контексте обработки для осуществления коммерческой деятельности, инициированной предоставлением продуктов и услуг заказчику;
- обязательные инструкции, раскрытие обрабатываемых данных и выполнение юридических обязательств;
- реализация технических и организационных мер;
- удаление персональных данных, которое должно быть согласовано в договоре;
- информация о субпроцессорах;
- некоторые дополнительные советы "на заметку".

Из руководства исключены темы международной передачи данных и экстерриториальной сферы применения законов США. Наконец, в руководстве отмечается, что оно не заменяет оценку защиты данных всех технических функций Microsoft 365, и ответственное лицо должно самостоятельно проводить проверку защиты данных.

<https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/einsatz-von-microsoft-365-praxis-tipps-fur-vertrage-mit-microsoft-225722.html>

<https://lfd.niedersachsen.de/download/199434>

## DPA: Бельгийский APD – соглашение об обработке данных не может применяться задним числом



Autorité de protection des données  
Gegevensbeschermingsautoriteit

1/16

Chambre Contentieuse

Décision quant au fond 137/2023 du 29 septembre 2023

Numéro de dossier : D05-2020-04511

Objet : Plainte relative à l'absence de contrat de sous-traitance (article 28.3. du RGPD) et à l'absence d'information suffisante par une autorité publique (article 14 du RGPD)

La Chambre Contentieuse de l'Autorité de protection des données, constituée de monsieur Hielke Hijmans, président, et de messieurs Romain Robert et Christophe Boeraeve, membres;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), ci-après "RGPD";

Vu la Loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après LCA);

Vu le règlement d'ordre intérieur tel qu'approuvé par la Chambre des représentants le 20 décembre 2018 et publié au Moniteur belge le 15 janvier 2019;

Vu les pièces du dossier;

A pris la décision suivante concernant :

Le plaignant : Monsieur X, ci-après : "le plaignant";

Les défenderesses : La commune Y1, ci-après : « la première défenderesse »;

La société Y2, représentée par Maître Louis Leurquin, avocat, dont le cabinet est établi avenue Brugmann, 435 à 1180 Bruxelles (Uccle), ci-après : "la seconde défenderesse";

Ci-après désignées ensemble comme « les défenderesses ».

Бельгийский надзорный орган (APD) отметил, что ст.28(1) GDPR обязывает обработчика предоставлять достаточные гарантии для защиты прав субъектов данных. Ст.28(3) GDPR обязывает контролеров заключать соглашение об обработке данных (DPA). Включение в соглашение оговорки о ретроактивности не исправляет отсутствие договора на момент события. Такой допуск позволил бы обойти применение обязательств ст.28(3) GDPR, направленных на обеспечение защиты прав и свобод субъектов данных. APD пришел к выводу, что как контроллер, так и обработчик несут ответственность за своевременное заключение соглашения об обработке данных.

## DPA: Соглашение о переходе с EU-US Privacy Shield на SCC-P в рамках дела Schrems II

RPPA (rppa.ru) Template EU-US Privacy Shield to SCC  
Amendment for Controller to Processor Transfer

### EU-US PRIVACY SHIELD TO SCC AMENDMENT FOR CONTROLLER TO PROCESSOR TRANSFER

This EU-US Privacy Shield to SCC Amendment for Controller to Processor Transfer (the **Amendment**) is concluded on «AmendmentDate» between:

1. «**ControllerName**», a company incorporated under the laws of «ControllerIncorpJurisdiction», with registration number «ControllerRegNo», whose legal address is «ControllerRegAddress» (hereinafter **Controller**); and
2. «**ProcessorName**», a company incorporated under the laws of «ProcessorIncorpJurisdiction», with registration number «ProcessorRegNo», whose legal address is «ProcessorRegAddress» (hereinafter **Processor**)

hereinafter referred to jointly as the **Parties** and separately as the **Party**.

#### 1. RECITALS

- 1.1. WHEREAS Controller and Processor are engaged in contractual relationship(s) which provide for certain transfer of personal data subject to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).
- 1.2. WHEREAS Controller and Processor previously concluded several agreements listed in Annex 1 to this Amendment covering the transfer of personal data mentioned in Section 1.1 above (the hereinafter referred to jointly as the **Underlying Agreements** and separately as the **Underlying Agreement**).
- 1.3. WHEREAS on 16 July 2020 (the **Effective Date**) the Court of Justice of the European Union in Case C-311/18 invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield.
- 1.4. WHEREAS Controller and Processor wish to enter into an agreement compliant with obligations under Articles 44-50 GDPR in order to continue their relationship(s) referred to in Section 1.1 above and to ensure that data subjects whose personal data are transferred to pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union.
- 1.5. NOW THEREFORE the Parties hereto agree as follows.

#### 2. AMENDMENTS

- 2.1. The Parties agree to amend the Underlying Agreements, including any data processing agreements or other instruments concluded in accordance with Article 28 GDPR or relevant provisions of earlier acts (as if) incorporated into Underlying Agreements, as follows:
  - 2.1.1. Any references to "Decision 2016/1250", "EU-U.S. Privacy Shield" and similar references to adequacy of protection afforded by the United States as a basis for international transfer outside of EEA are deemed excluded and the Underlying Agreements amended *mutatis mutandis*.
  - 2.1.2. The Parties agree to add the following wording to each of the Underlying Agreements:

*\*Start of wording\**

This agreement (contract or other form of contractual instrument) hereby incorporates by reference and gives effect to the contractual clauses annexed to the Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of

2 / 8

Типовой проект соглашения о переходе с условий EU-US Privacy Shield на Standard Contractual Clauses (Controller-to-Processor), подготовленный участником Russian Privacy Professionals Association - Олегом Блиновым.



## Court of Justice of the European Union

*Judgment in Case C-210/16  
Decision on 5 June 2018*

*Wirtschaftsakademie Schleswig-Holstein*

Администратор группы в Facebook совместно с самой социальной сетью является контролером обрабатываемых данных посетителей страницы и несет ответственность за их обработку.

*Judgment in Case C-25/17  
decision on 10 July 2018  
Tietosuojaalvautettu*

Религиозное объединение совместно с членами своих общин является контролером персональных данных, обрабатываемых в ходе проповеднической деятельности «от двери к двери», посредством которой члены общин, участвующие в проповедовании, распространяют веру своей общины. Хотя собранные персональные данные могут не передаваться религиозному объединению, но оно организывает, координирует и поощряет проповедническую деятельность своих общин.

РЕПУБЛИКА БЪЛГАРИЯ  
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Начало Институцията Правна рамка Практика Бъдете информирани Контакти

Администратори на лични данни  
Подаване на жалби и сигнали  
Въпроси към КЗЛД  
Международно сътрудничество  
Шенгенско пространство  
Анкета

ПРАКТИЧЕСКИ ВЪПРОСИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ СПЕД 25 МАЙ 2018 Г.

10 ПРАКТИЧЕСКИ СЪПЪЛКИ ЗА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ДАННИТЕ

Информационни технологии

Становище на КЗЛД по искане на „УниКредит Булбанк“ АД във връзка с прилагането на Регламент (ЕС) 2016/679

СТАНОВИЩЕ НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ рег. № НДМСПО-01-873/10.08.2018 г. гр. София, 21.09.2018 г.

ОТНОСНО: Искане за становище по прилагането на Регламент (ЕС) 2016/679 от „УниКредит Булбанк“ АД

Комисията за защита на личните данни (КЗЛД) в състав – членове: (целиели Софрониев, Мария Йатеева и Веселин Целеков, на заседание, проведено на 19.09.2018 г., разгледа искане за становище /вх. № НДМСПО-01-873/10.08.2018 г./ от „УниКредит Булбанк“ АД, в което са поставят следните въпроси относно прилагането на Регламент (ЕС) 2016/679:

1. Допустимо ли е съвместни администратори да разчитат на едно възникващо за предоставяне на съгласие от страна на субекта, чиито данни обработват, с цел предлагане на директен маркетинг.
2. Какво качество има банката във връзка с противоречивото тълкуване на сравните фигури „администратор“ и „обработващ лични данни“ в контекста на взаимнопорочията и с коментите.

Във връзка с прилагането на дейността си в съответствие с Регламент (ЕС) 2016/679, „УниКредит Булбанк“ АД се сблъсква с противоречиво тълкуване от страна на своите клиентинкоачеството на страните в отношенията, свързани с предоставяне на банкови услуги – администратор и обработващ. Клиентина банката изискват подписването на споразумение, според което клиентът има качеството на администратор по отношение на данните, които предоставя на „УниКредит Булбанк“ АД, въпреки, че банката има качеството обработващ данните. Основният им аргумент в тази насока е, че съдържанията между страните/договори за банкови услуги, по които клиентът има качеството „възложител“, а „УниКредит Булбанк“ АД на „изпълнител“, обуславят и поставянето им в позиция „администратор“ (клиент) и „обработващ“ (банката).

От своя страна, „УниКредит Булбанк“ АД не споделя това тълкуване на Общия регламент, като счита, че при осъществяването на дейността по предоставяне на банкови услуги на физически и юридически лица, тя притежава качеството/задълженията на „администратор“ на собствено основание по отношение на събираните и обработваните лични данни. В допълнение, предоставянето на тези специфични услуги може да бъде извършено единствено при наличие на съответния лиценз, т.е. обработването на данни се извършва на собствено основание, а не от името на клиента.

Политика за прозрачност  
Годишни отчети  
Информационен бюлетин  
Профил на купувача  
Административно обслужване  
Медии

Съобщения  
Информационна кампания  
По жалби  
Търсене

Календар на събитията  
Июни 2018  
П Н С Ч П С Н  
01 02 03 04  
05 06 07 08 09 10 11  
12 13 14 15 16 17 18  
19 20 21 22 23 24 25  
26 27 28 29 30

Архив  
Събития  
Фото галерия  
Конференции 2015  
Конкурс за дъща  
Наредба № 1 от 30 януари 2013 - отменяна, отменен от 25.05.2018  
Списъци, свързани с

## Комисията за защита на личните данни

Българският надзорен орган КЗЛД публикува свой отговор на запитване от банката „УниКредит Булбанк“, в който препоръчва сключване на договор за съвместно управление на данни. В договора трябва да бъдат определени задълженията на всяка от страните по спазване на изискванията на GDPR (особено в отношение на механизма на реализация на правата на субектите и задълженията по уведомление на субектите). Освен това, информацията за сключването на такъв договор и неговият съдържание трябва да бъдат предоставени на субектите на данни.

# DMA: Projekt Joint Controllers Agreement и образец уведомления субъектов о JCA от LfDI Baden-Württemberg



Landesbeauftragter für  
Datenschutz und  
Informationsfreiheit  
Baden-Württemberg

## Mehr Licht! – Gemeinsame Verantwortlichkeit sinnvoll gestalten

Gepostet von Pressestelle | 22. Mai 2019 | Aktuelle Meldungen, Datenschutz, Pressemitteilung



Die im letzten Jahr ergangenen Entscheidungen des Europäischen Gerichtshofes über die gemeinsame Verantwortlichkeit waren ein lauter Paukenschlag, deren Hall seitdem nicht verklungen ist. Die Rechtsfigur der „gemeinsamen Verantwortlichkeit“ und die damit verbundene Frage, wie eine solche vertragliche Vereinbarung zwischen den beteiligten Verantwortlichen eigentlich auszugestalten ist, löst seitdem bei vielen Verantwortlichen große Fragezeichen aus. Den gemeinsam Verantwortlichen kommt hierbei eine für den Betroffenen Schutz zentrale Aufgabe zu: Entscheiden mehrere Verantwortliche gemeinsam über Zwecke und Mittel der Datenverarbeitung, so sind sie gemeinsam verantwortlich und müssen untereinander vereinbaren, wer im Innenverhältnis welcher Pflicht aus der Datenschutz-Grundverordnung (DS-GVO) nachkommt.

Von offizieller aufsichtsbehördlicher Seite entwickelte Muster eines solchen Vertragswerks sucht man bislang vergeblich, so dass die Gestaltung eines solchen Vertrages den Vertragspartnern oftmals wichtige Zeit und personale Ressourcen raubt.



Landesbeauftragter für  
Datenschutz und  
Informationsfreiheit  
Baden-Württemberg

### Vereinbarung gemäß Art. 26 Abs. 1 S. 1 Datenschutz-Grundverordnung (DS-GVO) zwischen

**Partei 1**

**[Name und Kontaktdaten angeben]**

und

**Partei 2**

**[Name und Kontaktdaten angeben]**

*Hinweis: Dem vorliegenden Vertragsmuster liegen die Definitionen und Begriffe der Art. 4 und 5 DS-GVO zugrunde. Der Mustertext ist auf eine Vereinbarung zwischen zwei Vertragsparteien ausgelegt. Je nach Einzelfall können auch mehrere Vertragsparteien von einer gemeinsamen Verantwortlichkeit umfasst sein. In diesen Fällen muss das nachfolgende Muster insoweit auf eine größere Anzahl von Vertragsparteien umgeschrieben und angepasst werden.*

*Im Rahmen der durch den LfDI Baden-Württemberg durchgeführten Beratung zu Vertragsgestaltungen hat sich die in diesem Vertragsmuster vorgenommene Unterscheidung in Wirkbereiche als praktikabel erwiesen, auch wenn diese für eine wirksame Vereinbarung im Sinne des Art. 26 Abs. 1 DS-GVO nicht zwingend erforderlich ist.*

§ 1

(1) Diese Vereinbarung regelt die Rechte und Pflichten der Verantwortlichen (in Folge auch „Parteien“ genannt) bei der gemeinsamen Verarbeitung personenbezogener Daten. Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Beschäftigte der Parteien oder durch sie beauftragte Auftragsverarbeiter personenbezogene Daten für die Verantwortlichen verarbeiten. Die Parteien haben die Mittel und Zwecke der nachfolgend näher beschriebenen Verarbeitungstätigkeiten gemeinsam festgelegt.

## DMA: признание провайдера облачных услуг и его клиента в качестве Joint Controllers и требование заключить JCA

Številka: 0612-23/2019/19  
Datum: 1. 6. 2022

Informacijski pooblaščenec (v nadaljevanju IP) obuja po državni nadzornici za varstvo osebnih podatkov ... na podlagi 2. in 6. člena Zakona o informacijskem pooblaščenecu (Uradni list RS, št. 113/03 in 51/07 - ZUPB-A, v nadaljevanju: ZUPB); 37. in 54. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07-LPBBT in 17/20, v nadaljevanju: ZVOP-1), petega odstavka 28. in prvega odstavka 32. člena Zakona o informacijskem nadzoru (Uradni list RS, št. 43/07 - LPBBT in 40/14, v nadaljevanju: ZNA), ter člena 58(2) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter razveljavljuje Direktivo 95/46/ES (Splošna uredba o varstvu podatkov, v nadaljevanju: Splošna uredba), v zvezi s pritožbo inženjerskega podjetja na izvajanje storitev Splošne uredb in ZVOP-1 (pri zavezanecih ... (v nadaljevanju: zavezanec) po uradni dolžnosti naslednje:

**OBLOČBO**

- I. Zavezanec mora zavrati ugotovljenih nepravilnosti v zvezi s izvajanjem obločbe Splošne uredb z uporabniki (uporabljivo) ... uredbi razmerja z medsebojnim dogovorom v skladu s členom 28 Splošne uredb (skupni upravljanje).
- II. Ukrep iz I. točke uredbi te obločbe mora zavezanec izvršiti v roku 60 (šestdeset) dni od prejema te obločbe.
- III. Zavezanec mora o izvršenem ukrepu iz I. točke uredbi te obločbe v roku 5 (pet) dni po izvršitvi pisno obvestiti IP in predložiti dokazila.
- IV. V tem postopku posebni stroški niso nastali.

**Obravnavilitev**

- I. Precessata dejanja, ugotovljiva IP in navedbe zavezanca

IP vodi zoper zavezanca postopek informacijskega nadzora, s okviru katerega preverja obdelavo osebnih podatkov v okviru ...

V okviru predmetnega postopka je IP:

- dne 5.2.2019 pozval zavezanca na posredovanje pisnega pojasnila, dokumentacije in izjave (skl. št. 0612-23/2019/19), na katerega je zavezanec odgovoril z dopisoma št. 071-7201714 dne 22.3.2019 in št. 071-7201716 dne 27.3.2019, ki jima je priložil relevantno dokumentacijo v zvezi s sistemom ... in sklenil odgovoriti na vprašanja glede zagotavljanja informacijske varnosti v zvezi z izvajanjem storitve ... Akt o organizaciji delovanja ... Načrti, podatkov ... Akt o postopkih in ukrepih za zmanjševanje osebnih podatkov v ... Navodilo o uporabi ... sredstev. Navodilo za uporabo ... celotno silo izvajanja storitve.

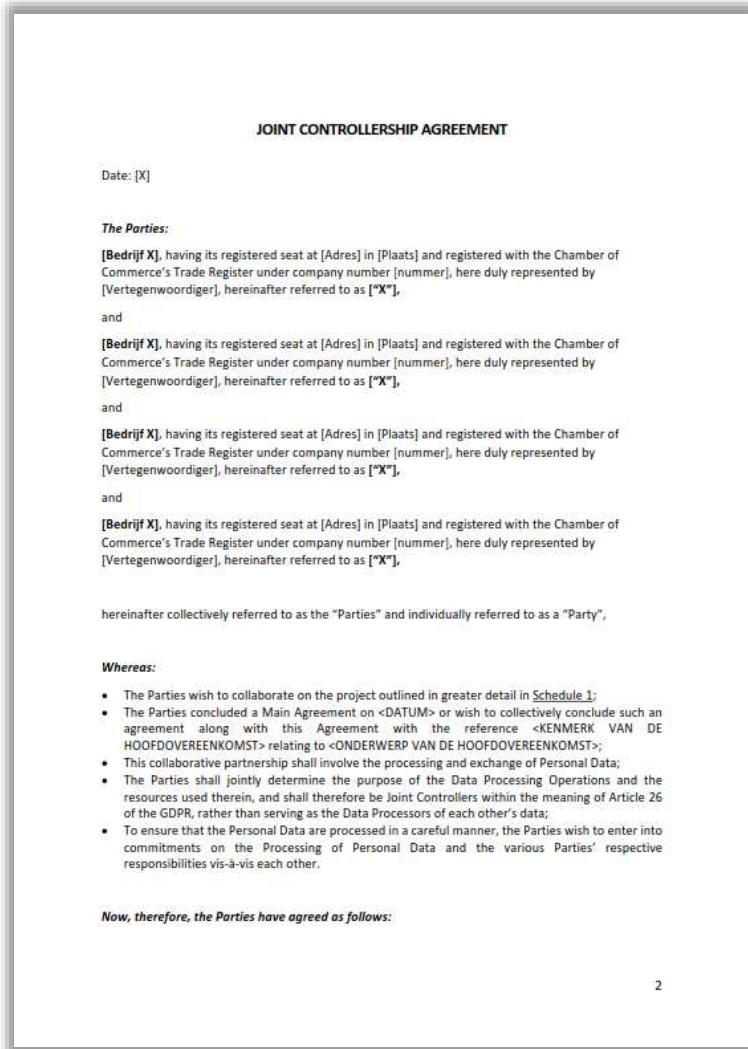
Надзорный орган по защите данных Словении инициировало расследование в отношении компании, которая выступала в качестве посредника между клиентами, генерирующими запросы на данные, и различными провайдерами данных. Компания утверждала, что клиенты, запрашивающие данные, являются контролерами и что она просто обрабатывает данные от имени этих клиентов/контролеров.

Словенский DPA установил, идея бизнес-модели облачных вычислений заключалась в обработке сложных технических деталей с целью упростить технические аспекты для клиентов, позволяя им полностью сосредоточиться на содержании запрашиваемых данных. Пользователи облачных вычислений практически не влияли на технические и организационные меры, применяемые провайдером облачных вычислений при обработке данных.

Поскольку клиенты провайдера облачных вычислений не имели возможности обеспечить техническое соответствие GDPR, провайдер облачных вычислений выступал в качестве контролера, поскольку он определял технические процессы, с помощью которых данные запрашивались, обрабатывались и передавались, а также то, какие субпроцессы были привлечены.

Так как провайдер облачных вычислений и его клиенты вместе определяли цели и средства обработки, их соглашение фактически было совместным контролем на обработкой данных. DPA постановил, что провайдер услуг облачных вычислений должен регулировать свои договоренности с клиентами по взаимному соглашению в соответствии со ст.26 GDPR (совместные контролеры).

## DMA: Data Management Agreement как оптимальный способ регулирования оборота данных в холдинге



**Model Joint Controllership Agreement or SURF:**  
<https://www.surf.nl/files/2019-11/model-joint-controllership-agreement.pdf>

В каких случаях может потребоваться DMA (JCA):

1. совместное определение цели в отношении обработки персональных данных;
2. использование одного и того же набора персональных данных (или базы данных) для достижения общей цели;
3. совместное определение облика процесса обработки персональных данных, пусть и с разными целями;
4. наличие общих правил управления персональными данными.

Некоторые преимущества DMA для холдинга:

- ✓ установление иерархичности сторон и порядка принятия решений;
- ✓ гибкое распределение ответственности между участниками;
- ✓ централизованное взаимодействие холдинга с процессорами и субпроцессорами;
- ✓ использование для экспорта данных из ЕС/ЕАСТ посредством SCC-C;
- ✓ возможность учесть особенности права, применимого к участникам, находящимся вне ЕС/ЕАСТ;
- ✓ отсутствие механизма обязательного согласования с надзорными органами.





European Commission

English Search

Home > ... > International dimension of data protection > Binding Corporate Rules (BCR)

### Binding Corporate Rules (BCR)

Corporate rules for data transfers within multinational companies.

#### What are binding corporate rules?

Binding corporate rules (BCR) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every member concerned of the group.

#### Approval of binding corporate rules

Companies must submit binding corporate rules for approval to the competent data protection authority in the EU. The authority will approve the BCRs in accordance with the consistency mechanism set out in Article 63 of the [GDPR](#). This procedure may involve several supervisory authorities since the group applying for approval of its BCRs may have entities in more than one Member State. The competent authority communicates its draft decision to the European Data Protection Board, which will issue its opinion on the binding corporate rules. When the BCRs have been finalised in accordance with the EDPB opinion, the competent authority will approve the BCRs.

Authorisations of supervisory authorities on the basis of Directive 95/46/EC remain valid until amended, replaced or repealed, if necessary, by that supervisory authorities.

Рекомендации Рабочей группы по защите физических лиц при обработке персональных данных ([Data Protection Working Party, WP29](#)), которая действовала до 25.05.2018. [Некоторые](#) из указанных рекомендаций продолжают действовать после расформирования Рабочей группы WP29 и передачи полномочий Европейскому совету по защите данных:

1. [Explanatory Document on the Processor Binding Corporate Rules, WP 204 rev.01](#)
2. [Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP 263 rev.01](#)
3. [Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264](#)
4. [Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265](#)
5. [Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01](#)
6. [Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01](#)

## 282 BCR: Новые рекомендации EDPB по BCR-C



Европейский совет по защите данных (EDPB) объявил, что 15.11.2022 принял Рекомендации 1/2022 о заявке на утверждение и об элементах и принципах, которые должны содержаться в обязательных корпоративных правилах контроллера, которые будут подлежать публичным консультациям до 10.01.2023. EDPB отметил, что Рекомендации представляют собой обновление существующего справочника "Обязательные корпоративные правила контролеров" ("BCR-C"), который содержит критерии для утверждения BCR-C, и объединяют его со стандартной формой заявления для утверждения BCR-C.

Проект Рекомендаций основан на договоренностях, достигнутых органами по защите данных ЕС в ходе процедур утверждения заявок на конкретные корпоративные обязательные правила ("BCRs") после вступления в силу GDPR, и приводят существующее руководство в соответствие с требованиями постановления Суда Европейского союза ("CJEU") по делу Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) ("дело Schrems II").

Отдельно EDPB подтвердил, что в настоящее время разрабатывается второй набор рекомендаций по BCR для процессоров.

## 283 BCR: Почему же так мало утвержденных BCR?



### Некоторые из компаний-участников BCR до 2018г.:

ABN AMRO Bank	Cisco	Legrand
Airbus	Citigroup	Maersk Group
Allianz	Deutsche Post DHL	Mastercard
Astra Zeneca plc	Deutsche Telekom	Michelin
American Express	e-Bay	Motorola
ArcelorMittal Group	Ericsson	Novartis
AVAYA Group	Ernst & Young	Oracle
BMW	General Electric	Osram
BNP Paribas	Hewlett Packard	PayPal
BP	IBM Corporation	Salesforce
BT Group	Intel Corporation	Schneider Electric
Cargill	John Deere	Siemens

Name of the group of undertakings/entities -	Type of BCRs (controller or processor)	Year of approval/last update	Approved	Categories of data subjects	
BCRs of Equinix Inc.	Controller	2019	UK SA	Employees and business contacts	<a href="#">View details</a>
BCRs of ExxonMobil Corporation	Controller	2019	BE SA	Employees and business contacts	<a href="#">View details</a>
BCRs of Fujikura Automotive Europe Group (FAE Group)	Controller	2020	ES SA	Employees and business contacts	<a href="#">View details</a>

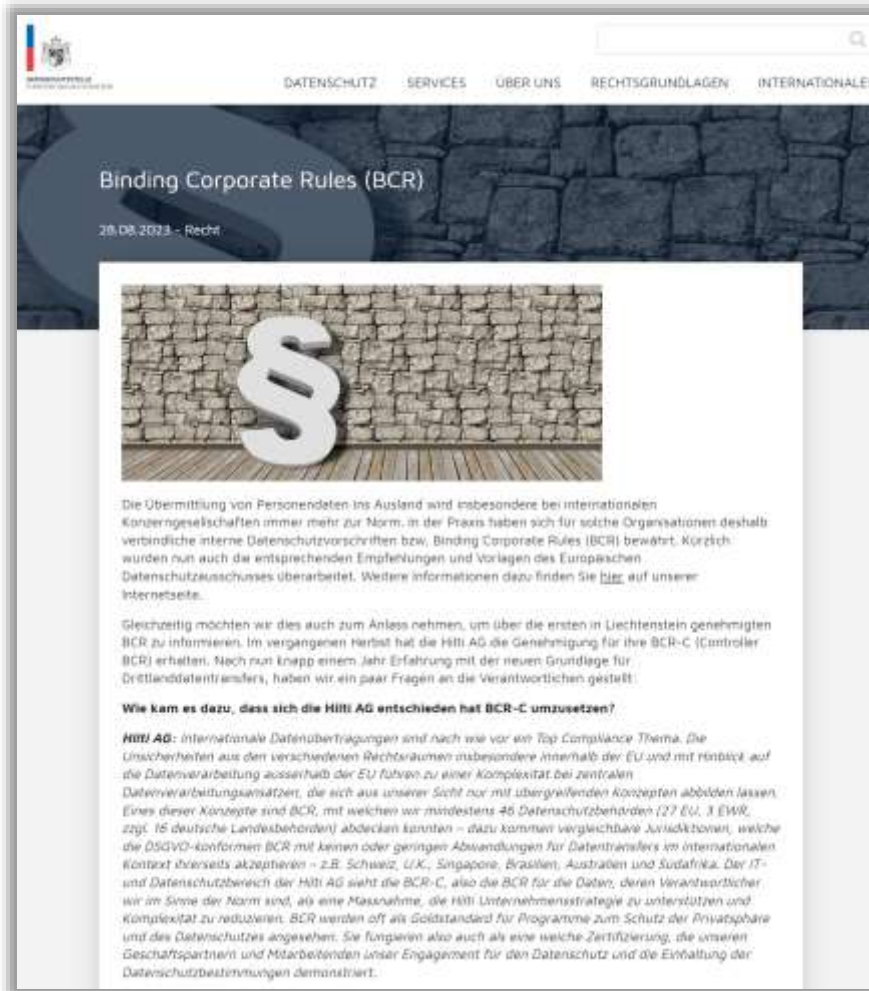
### Некоторые из компаний-участников BCR с 2019г.:

ExxonMobil  
Equinix  
Fujikura Automotive Europe Group Reinsurance  
Group of America  
Tetra Pak  
COLT Group  
Luxoft Group  
Otis  
Saxo Bank Group  
Daimler Truck Group  
Mercedes Benz Group

[https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=613841](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841)


[https://edpb.europa.eu/our-work-tools/accountability-tools/bcr\\_en](https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en)

## BCR: Заметка лихтенштейнского DSS о первом одобренном в Лихтенштейне BCR-C



Binding Corporate Rules (BCR)

28.08.2023 - Recht



Die Übermittlung von Personendaten ins Ausland wird insbesondere bei internationalen Konzerngesellschaften immer mehr zur Norm. In der Praxis haben sich für solche Organisationen deshalb verbindliche interne Datenschutzvorschriften bzw. Binding Corporate Rules (BCR) bewährt. Kürzlich wurden nun auch die entsprechenden Empfehlungen und Vorlagen des Europäischen Datenschutzausschusses überarbeitet. Weitere Informationen dazu finden Sie [hier](#) auf unserer Internetseite.

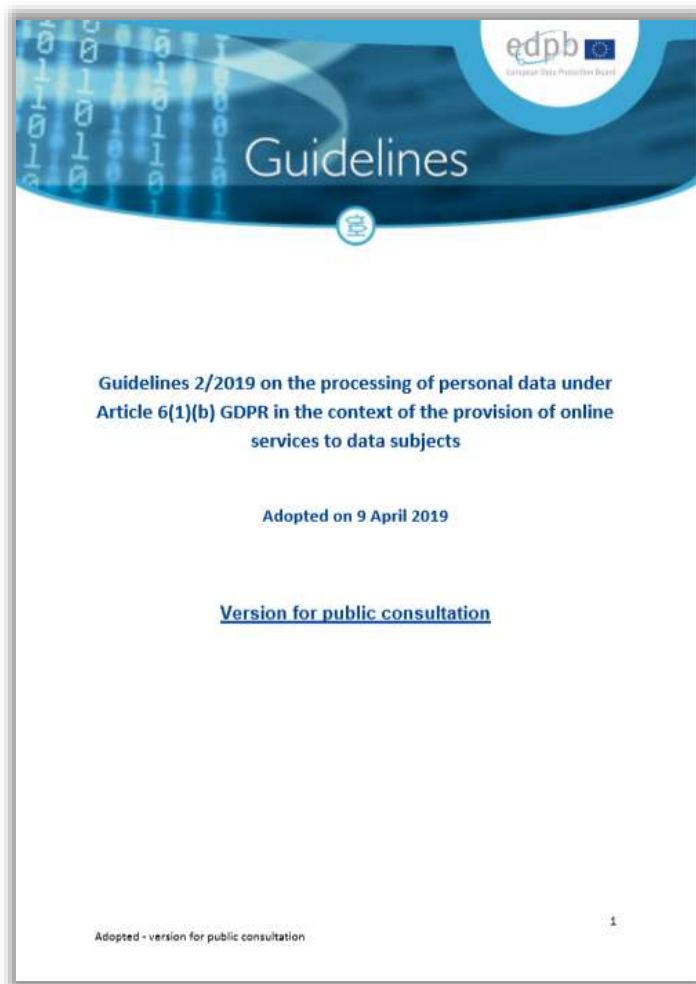
Gleichzeitig möchten wir dies auch zum Anlass nehmen, um über die ersten in Liechtenstein genehmigten BCR zu informieren. Im vergangenen Herbst hat die Hilti AG die Genehmigung für ihre BCR-C (Controller BCR) erhalten. Nach nur knapp einem Jahr Erfahrung mit der neuen Grundlage für Drittlanddatentransfer, haben wir ein paar Fragen an die Verantwortlichen gestellt:

**Wie kam es dazu, dass sich die Hilti AG entschieden hat BCR-C umzusetzen?**

**Hilti AG:** Internationale Datenübertragungen sind nach wie vor ein Top-Compliance-Thema. Die Unsicherheiten aus den verschiedenen Rechtsräumen insbesondere innerhalb der EU und mit Hinblick auf die Datenverarbeitung ausserhalb der EU führen zu einer Komplexität bei zentralen Datenverarbeitungsansätzen, die sich aus unserer Sicht nur mit übergreifenden Konzepten abbilden lassen. Eines dieser Konzepte sind BCR, mit welchen wir mindestens 45 Datenschutzbehörden (27 EU, 3 EWR, zzgl. 15 deutsche Landesbehörden) abdecken könnten – dazu kommen vergleichbare Jurisdiktionen, welche die DSGVO-konformen BCR mit keinen oder geringen Abweichungen für Datentransfer im internationalen Kontext diversivets akzeptieren – z.B. Schweiz, UK, Singapur, Brasilien, Australien und Südafrika. Der IT- und Datenschutzbereich der Hilti AG sieht die BCR-C, also die BCR für die Daten, deren Verantwortlicher wir im Sinne der Norm sind, als eine Massnahme, die Hilti Unternehmensstrategie zu unterstützen und Komplexität zu reduzieren. BCR werden oft als Goldstandard für Programme zum Schutz der Privatsphäre und des Datenschutzes angesehen. Sie fungieren also auch als eine welche-Zertifizierung, die unseren Geschäftspartnern und Mitarbeitenden unser Engagement für den Datenschutz und die Einhaltung der Datenschutzbestimmungen demonstriert.

28.08.2023 орган по защите данных Лихтенштейна (DSS) опубликовал заметку, посвященную обязательным корпоративным правилам для контролеров (BCR-C) компании Hilti AG, которые стали первыми в истории BCR, утвержденными DSS в 2022 году. В заметке рассказывается о том, как Hilti AG внедрила BCR-C для передачи данных в третьи страны, в том числе о том, как компания тесно сотрудничала с DSS в процессе разработки и утверждения.

## SPA: Руководство EDPB по обработке персональных данных при предоставлении онлайн-услуг субъектам



Это руководство призвано помочь в определении правового основания обработки персональных данных в контексте заключаемых с субъектами данных контрактов на оказание им онлайн-услуг, независимо способа оплаты данных услуг. В руководстве изложены квалифицирующие признаки правомерной обработки персональных данных в соответствии со ст.6(1)(b) GDPR и рассмотрена концепция «необходимости» в том виде, в каком она применима к исполнению контракта.

На что необходимо обратить дополнительное внимание в контексте договорной деятельности с субъектами:

- ✓ После расторжения контракта обычно несправедливо переходить на другое легальное основание (п. 41).
- ✓ Действия, связанные с контрактом после его расторжения (возврат оплаты и т.п.) тоже могут быть основаны на статье 6(1)(b). (п. 42, 44).
- ✓ Обычно контракт с клиентом не является основанием для демонстрации ему таргетированной рекламы. Но если хочется, нужно учесть, что клиент имеет право возражать против прямого маркетинга по статье 21 GDPR (п. 52), учесть требования ePrivacy, мнение по WP171 и WP208 (п. 55).
- ✓ Персональные данные не могут рассматриваться в качестве коммерческого товара (п. 54).

## SPA: Руководство DPC по определению правовой основы для обработки персональных данных

Version last updated: December 2019

### Contract

"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

Article 6(1)(b) GDPR

The legal basis of 'contract' (also referred to as 'contractual necessity' or 'contractual performance') is another relatively commonly utilised legal basis for the processing of personal data, in contexts where there is a **contractual relationship** between the **data subject and the controller**. Article 6(1)(b) and Recital 44 GDPR set out that processing may be lawful where necessary for performing or initiating a valid contract.

Controllers need to be aware that to rely on a contractual legal basis for processing personal data it isn't sufficient for the processing to just be somehow related to the contractual relationship, instead it must go further and be **'necessary for the performance'** of that contract – i.e. objectively necessary to carry out the contract. Alternatively, this legal basis may be relied upon where the processing is necessary to **take steps** leading towards a contract, where the data subject has requested the controller do so, as discussed in more detail below.

As set out in the wording of Article 6(1)(b) GDPR, controllers need to be aware that this legal basis can only apply to **contracts between the actual data subject and the controller**, and not to processing of personal data for the purpose of performing a contract between a controller and a third party. Thus, a controller cannot use a contract between themselves and another service provider or advertising partner as the legal basis for the processing of a data subject's personal data, just because the processing would be necessary to perform that contract – as the data subject is not a party to that contract. Thus, this legal basis would not apply in the **absence of a direct contractual relationship** with the data subject concerned.

#### Prior to Entering into a Contract

The wording of Article 6(1)(b) GDPR reflects the fact that preliminary processing an individual's personal data may be necessary before entering into a contract with the controller, in order to facilitate concluding a contract, such as the processing of personal details by an insurance company where a data subject has **asked for a quote**, with a view to potentially entering into a contract of insurance.

In an online context, this may be of relevance in situations where, for example, a data subject provides their postal address to see if a particular service provider operates in their area, or processing which is carried out as part of a registration process for an online service. This idea of preliminary processing **could not cover unsolicited marketing** or other processing which is carried out solely on the initiative of the controller, or at the request of a third party, as this isn't done at the request of the actual data subject.

Ирландский надзорный орган Data Protection Commission в декабре 2019 года опубликовал руководство для контролеров по определению правильной правовой основы для той или иной обработки персональных данных и обязательств, которые соответствуют этой правовой основе.

Страницы 11-13 руководства посвящены анализу базовых требований к обработке персональных данных в контексте преддоговорной и договорной деятельности между контролером и субъектом данных.

	Right of Access	Right to Rectification	Right to Erasure	Right to Restriction	Right to Portability	Right to Object
Consent	✓	✓	✓	✓	✓	~ Can withdraw consent
<b>Contract</b>	✓	✓	✓	✓	✓	✗
Legal Obligation	✓	✓	✗	✓	✗	✗
Vital Interests	✓	✓	✓	✓	✗	✗
Public Task	✓	✓	✗	✓	✗	✓
Legitimate Interests	✓	✓	✓	✓	✗	✓

## SPA: Subject's Privacy Addendum как необходимый элемент договора между контролером и субъектом данных

### Subject's Privacy Addendum (в качестве раздела в договор ГПХ с ФЛ)

1. Подписывая Договор, Исполнитель наделяет Заказчика, как самостоятельно действующего оператора (здесь и далее понятия «оператор», «персональные данные», «обработка персональных данных» используются в значении, определенном ст.3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»), правом на осуществление обработки персональных данных Исполнителя, с целью заключения, исполнения и прекращения Сторонами Договора, а также с целью осуществления, выполнения и соблюдения Сторонами прав, обязанностей и запретов, предусмотренных применимыми нормами. Состав персональных данных Исполнителя, подлежащих обработке, а также перечень действий (операций), совершаемых с персональными данными Исполнителя, определяются в соответствии с предусмотренными целями и условиями Договора.
2. В случае, если Исполнитель в предусмотренных целях передает Заказчику персональные данные иных субъектов персональных данных (далее – «субъекты»), то тем самым Исполнитель заверяет и гарантирует правомерность такой передачи персональных данных в соответствии с требованиями применимого законодательства, а также надлежащее уведомление субъектов о такой передаче их персональных данных Заказчику, если того требует применимое законодательство.
3. Для достижения предусмотренных целей обработки персональных данных Заказчик:
  - (1) вправе привлекать третьих лиц к обработке персональных данных путем поручения третьим лицам обработки персональных данных и (или) путем передачи третьим лицам персональных данных без поручения обработки персональных данных, в том числе осуществлять трансграничную передачу персональных данных третьим лицам на территорию Соединенных Штатов Америки, государств-членов Европейского союза и иных иностранных государств. Привлечение третьих лиц к обработке персональных данных может осуществляться только при условии обработки такими лицами персональных данных исключительно для достижения предусмотренных целей обработки персональных данных, а также при условии обеспечения такими лицами конфиденциальности и безопасности персональных данных при их обработке. К третьим лицам, в частности, относятся контрагенты Заказчика, а также аффилированные (в значении понятия, определенного ст.9 Федерального закона от 26.07.2006 № 135-ФЗ «О защите конкуренции») с Заказчиком компании;
  - (2) вправе обрабатывать персональные данные до момента окончания действия Договора, а также в течение 5 (пяти) лет после прекращения действия Договора для соблюдения сроков исковой давности и выполнения требований законодательства о налогах и о бухгалтерском учете, если иное не предусмотрено соглашением между Сторонами или применимым законодательством;
  - (3) обязуется обеспечивать конфиденциальность и безопасность персональных данных при их обработке в соответствии с требованиями применимого законодательства.
4. Для достижения предусмотренных целей обработки персональных данных Исполнитель:
  - (1) имеет право доступа к относящимся к нему персональным данным, требовать их уточнения, блокирования или уничтожения в случае, если такие персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки. Исполнитель может реализовать свое право через письменное обращение путем его личного представления представителю Заказчика или почтового направления по адресу Заказчика;
  - (2) обязуется предоставлять точные, полные и актуальные персональные данные для обработки в предусмотренных целях. В случае изменения относящихся к нему персональных данных Исполнитель обязуется своевременно и надлежащим образом уведомлять об этом Заказчика;
  - (3) обязуется не позднее 5 (пяти) рабочих дней со дня получения запроса от Заказчика предоставлять Заказчику сведения и (или) документы, подтверждающие либо факт получения согласия иных субъектов на осуществление передачи их персональных данных от Исполнителя к Заказчику, либо наличие иных правовых оснований для осуществления указанной передачи персональных данных субъектов и факт надлежащего уведомления субъектов о такой передаче их персональных данных;
  - (4) обязуется добросовестно сотрудничать с Заказчиком и оказывать Заказчику необходимое разумное содействие при рассмотрении и урегулировании запросов (жалоб, требований, предписаний, претензий, судебных исков), касающихся обрабатываемых на основании Договора персональных данных, полученных Заказчиком от Исполнителя.

- ✓ определяет статус организации в отношении с субъектом данных как самостоятельного контролера;
- ✓ фиксирует цели договорной обработки персональных данных – заключение, исполнение и прекращение сторонами договора, а также осуществление, выполнение и соблюдение Сторонами прав, обязанностей и запретов, предусмотренных применимыми нормами;
- ✓ вводит в договор необходимый понятийный аппарат;
- ✓ явно указывает на период пост-договорной обработки данных;
- ✓ вменяет контролеру в обязанность обеспечивать конфиденциальность и безопасность обработки персональных данных;
- ✓ защищает права и законные интересы субъекта при обработке персональных данных;
- ✓ позволяет контролеру привлекать третьих лиц к обработке полученных персональных данных;
- ✓ обязывает субъекта добросовестно сотрудничать с контролером и оказывать ему необходимое разумное содействие при рассмотрении и урегулировании запросов (жалоб, требований, предписаний, претензий, судебных исков), касающихся обрабатываемых на основании договора персональных данных.

Подготовленный автором презентации проект SPA, предназначенный для **договоров согласно праву РФ:**

<http://sps-ib.ru/spa.docx>

## SPA: Статья о надлежащей обработке и защите персональных данных в договорных отношениях согласно ст.6(1)(b) GDPR

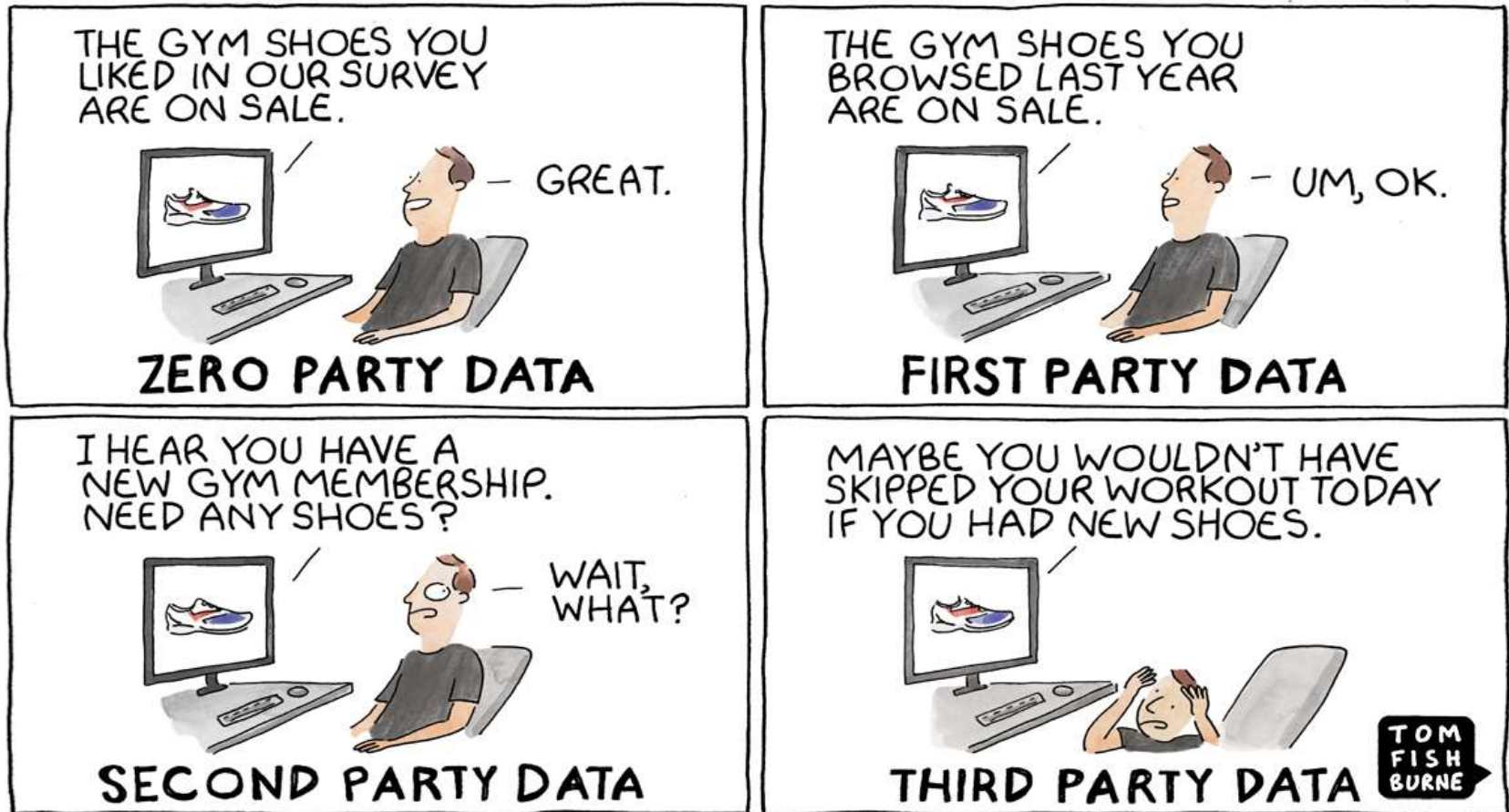
Table of Content	
<b>I. Subject, Scope and Research Question</b> .....	5
<b>II. The GDPR as an instrument of enabling and protection</b> .....	13
1. <i>Dual functionality of the GDPR: Freedom of data flows and data protection</i> .....	13
2. <i>Market regulation for personal data in compliance with the protection standard pursuant to Art. 8 (1) CFR</i> .....	19
3. <i>Necessity of interpreting Art. 6 (1) GDPR in light of its dual function</i> .....	22
4. <i>The GDPR as Market Regulation Law: Equal Value of Contract and Consent</i> .....	23
<b>III. The Construction of Data Protection: Right to arbitrary control or right to unharmed digital sociality?</b> .....	26
1. <i>Data protection law as part of an information order</i> .....	26
2. <i>Data protection as "control": Protection of the informational free will</i> .....	28
a) <i>Focus of data protection on information control</i> .....	29
b) <i>Individualism, data minimisation, anonymity</i> .....	30
c) <i>Weaknesses and deficits</i> .....	31
3. <i>Data protection and digital sociality: the function of data protection in society as a whole</i> .....	34
a) <i>Data privacy as an integral part of an information order</i> .....	35
b) <i>The basic structure of the GDPR</i> .....	40
c) <i>Socially integrated and self-determined life in a digital society</i> .....	42
<b>IV. Data protection in contractual relationships: Art. 6 (1) (b) GDPR</b> .....	48
1. <i>Hierarchical position of Art. 6 (1) (b) GDPR in the system of justification grounds</i> .....	49
2. <i>Optimizing digital autonomy through contractual agreements</i> .....	50
a) <i>Contract, realization of preferences and bargaining power</i> .....	51
aa) <i>Contracts as expression of self-determination</i> .....	52
bb) <i>Ensuring substantive contractual autonomy</i> .....	54
cc) <i>Limitations of digital contractual autonomy</i> .....	56
dd) <i>Inappropriateness of data protection exceptionalism</i> .....	57
b) <i>EU Regulations to safeguard substantive contractual autonomy</i> .....	58
c) <i>No reason or authority for "choice-requiring paternalism"</i> .....	61
d) <i>No danger of unlimited commercialization</i> .....	65
3. <i>Optimization of fundamental rights values and legal positions</i> .....	66
a) <i>Necessity of taking all affected fundamental rights into account - inadmissibility of a silo-ed approach under data protection law</i> .....	66
b) <i>Entrepreneurial Freedom under Art. 16 CFR</i> .....	69
aa) <i>Protective scope</i> .....	69
bb) <i>Substantive Interference</i> .....	70
c) <i>Freedom of contract of the individual according to Art. 6 CFR</i> .....	72
3	
<small>Downloaded from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4427134</small>	

Ст.6(1)(b) GDPR предусматривает, что контролер действует обоснованно, если обработка персональных данных необходима для выполнения договора, стороной которого является субъект данных. В основе статьи за авторством Профессора Мартина Неттесхайма (юридический факультет Тюбингенского университета) лежит тезис о том, что надлежащая обработка и защита персональных данных в договорных отношениях может и должна быть реализована, прежде всего, за счет соответствующей конструкции договорных отношений.

Требование о получении согласия после заключения договора не только не укрепляет цифровую автономию субъектов данных, но и в конечном итоге способствует ее ослаблению. Уровень защиты, предусмотренный ст. 8 CFR, не может быть достигнут путем постоянного увеличения количества требований о согласии в цифровом мире - это приводит лишь к "усталости от согласия". В статье подробно описано, какие конкретные требования возникают в связи с этим для понимания ст.6(1)(b) GDPR.



# Интернет-ресурсы, профилирование и прямой маркетинг (реклама)



## Краткий обзор методов сбора данных о пользователях веб-сайтов и мобильных приложений



Cookies



Pixels



Fingerprinting



APIs



SDKs

### Definitions

- |   |  |  |   |  |
|---|--|--|---|--|
| <ul style="list-style-type: none"> <li>▶ A small file of data stored on a user's device via a web browser</li> <li>▶ Identifies and tracks users across websites</li> </ul> | <ul style="list-style-type: none"> <li>▶ A snippet of code on a website</li> <li>▶ Sends user data to third-parties</li> </ul> | <ul style="list-style-type: none"> <li>▶ A "fingerprint" of device or browser properties</li> <li>▶ Uniquely identifies a particular device</li> </ul> | <ul style="list-style-type: none"> <li>▶ Intermediary software that facilitates communication between two programs</li> <li>▶ Shares data and certain cross-functional tools</li> </ul> | <ul style="list-style-type: none"> <li>▶ Complete toolkit of software and code, often including APIs</li> <li>▶ Helps develop and integrate mobile apps with other services</li> </ul> |
|---|--|--|---|--|

### Providers

- |  |   |   |   |  |
|--|---|---|---|--|
| <ul style="list-style-type: none"> <li>▶ 1st-party cookies are created by a website visited by a user</li> <li>▶ 3rd-cookies are created by an entity other than the operator of the website a user is visiting</li> </ul> | <ul style="list-style-type: none"> <li>▶ Code is often provided by third-parties with ad services, primarily for targeted advertising</li> <li>▶ Code may be placed on a website by its operator</li> </ul> | <ul style="list-style-type: none"> <li>▶ Some third-parties provide fingerprinting and device identification services to websites</li> <li>▶ Some websites may also directly collect data for fingerprinting</li> </ul> | <ul style="list-style-type: none"> <li>▶ Certain APIs may be provided by large companies or included in SDKs</li> <li>▶ Access to APIs can be restricted by API-provider</li> </ul> | <ul style="list-style-type: none"> <li>▶ Certain SDKs may be provided by large companies for interoperability and data sharing</li> <li>▶ Some SDKs may be provided by the manufacturer of a hardware platform, operating system, or programming language</li> </ul> |
|--|---|---|---|--|

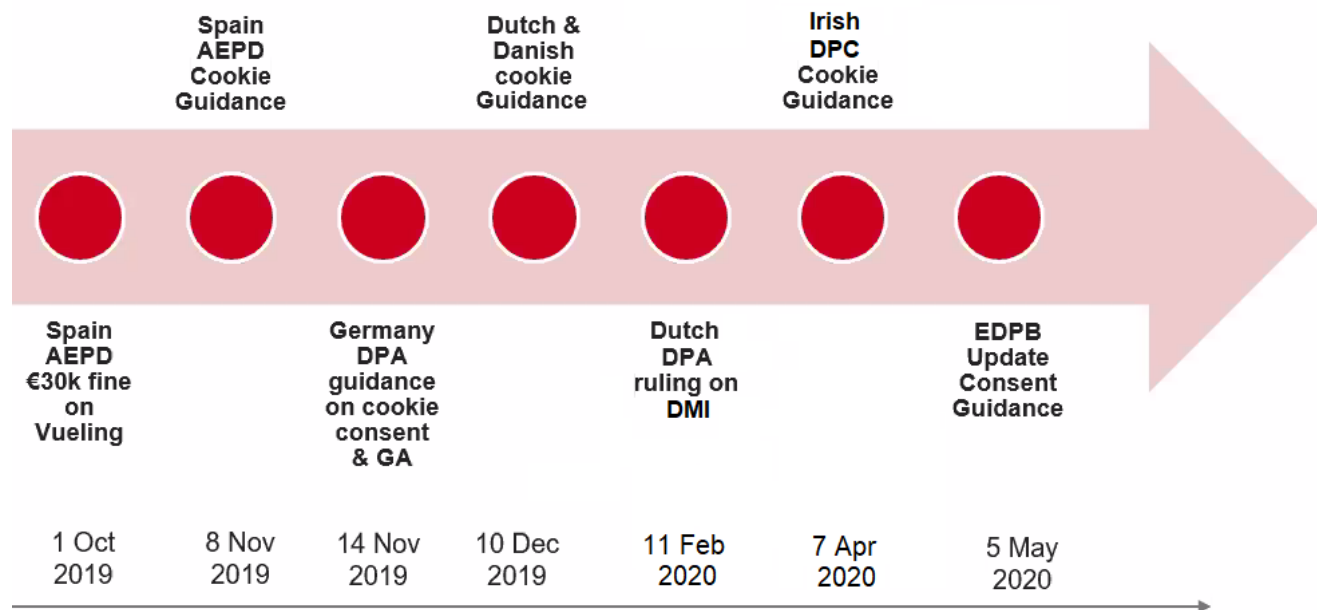
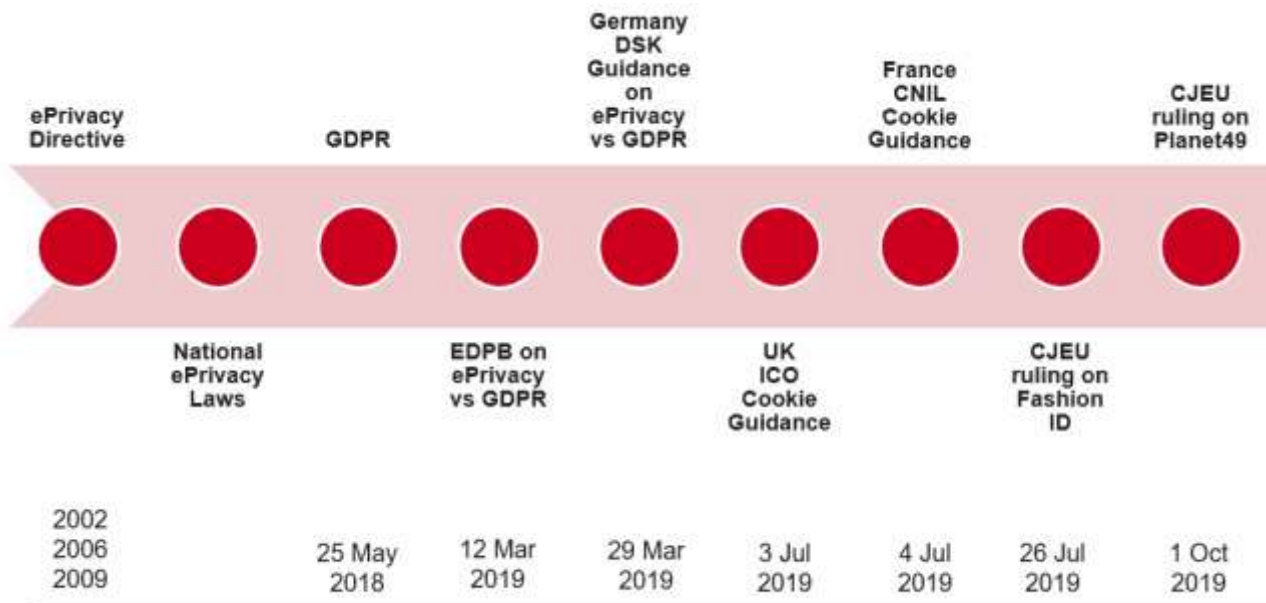
### Tracking & Anti-Tracking

- |  |   |   |   |   |
|--|---|---|---|---|
| <ul style="list-style-type: none"> <li>▶ May be banned by certain web browsers, such as Firefox or Safari</li> </ul> | <ul style="list-style-type: none"> <li>▶ May be used to evade web browser bans on cookies</li> <li>▶ May be interrupted by ad blockers</li> </ul> | <p>May be used to evade:</p> <ul style="list-style-type: none"> <li>▶ Web browser cookie bans</li> <li>▶ Ad blockers</li> <li>▶ VPNs</li> </ul> | <ul style="list-style-type: none"> <li>▶ Certain APIs may be used to evade ad blockers, since they are less impacted than pixels</li> </ul> | <ul style="list-style-type: none"> <li>▶ Certain SDKs—sometimes described as the mobile equivalent of cookies—can be included in mobile apps to collect data without a user's awareness</li> <li>▶ May be limited by restricting app requests to use device features or resetting ad IDs</li> </ul> |
|--|---|---|---|---|

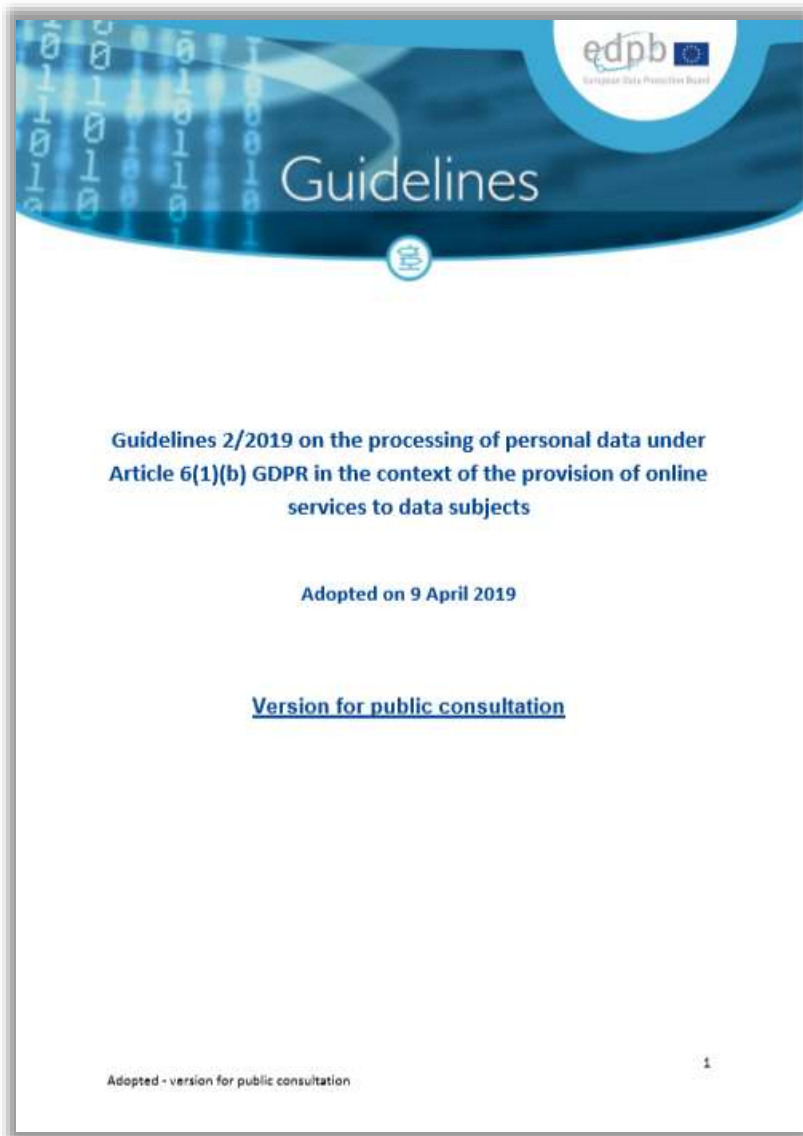
### Examples

- |  |  |  |  |  |
|--|--|--|--|--|
| <ul style="list-style-type: none"> <li>▶ Analytics cookies (e.g., Google Analytics cookies used to distinguish visitors for two years)</li> <li>▶ Advertising cookies (e.g., Cookies used by advertisers to measure performance of ads)</li> </ul> | <ul style="list-style-type: none"> <li>▶ Meta Pixel</li> <li>▶ TikTok Pixel</li> </ul> | <p>Fingerprint formed from data such as:</p> <ul style="list-style-type: none"> <li>▶ Screen size &amp; resolution</li> <li>▶ Browser information</li> <li>▶ Operating system details</li> </ul> | <ul style="list-style-type: none"> <li>▶ Analytics APIs provide website operators data about their visitors (e.g., Facebook's Ads Insights APIs)</li> <li>▶ Feature APIs allow websites and apps to integrate another service's feature into their own offering (e.g., API for Google search within a separate website)</li> </ul> | <ul style="list-style-type: none"> <li>▶ Analytics or Monetization SDKs (e.g., Google Mobile Ads SDK for Ad Manager; Firebase SDK for Google Analytics)</li> <li>▶ Platform or language-specific SDKs to develop apps (e.g., iOS SDK)</li> </ul> |
|--|--|--|--|--|

## Развитие регулирования cookies и аналогичных технологий отслеживания в ЕС в 2002-2020 годах



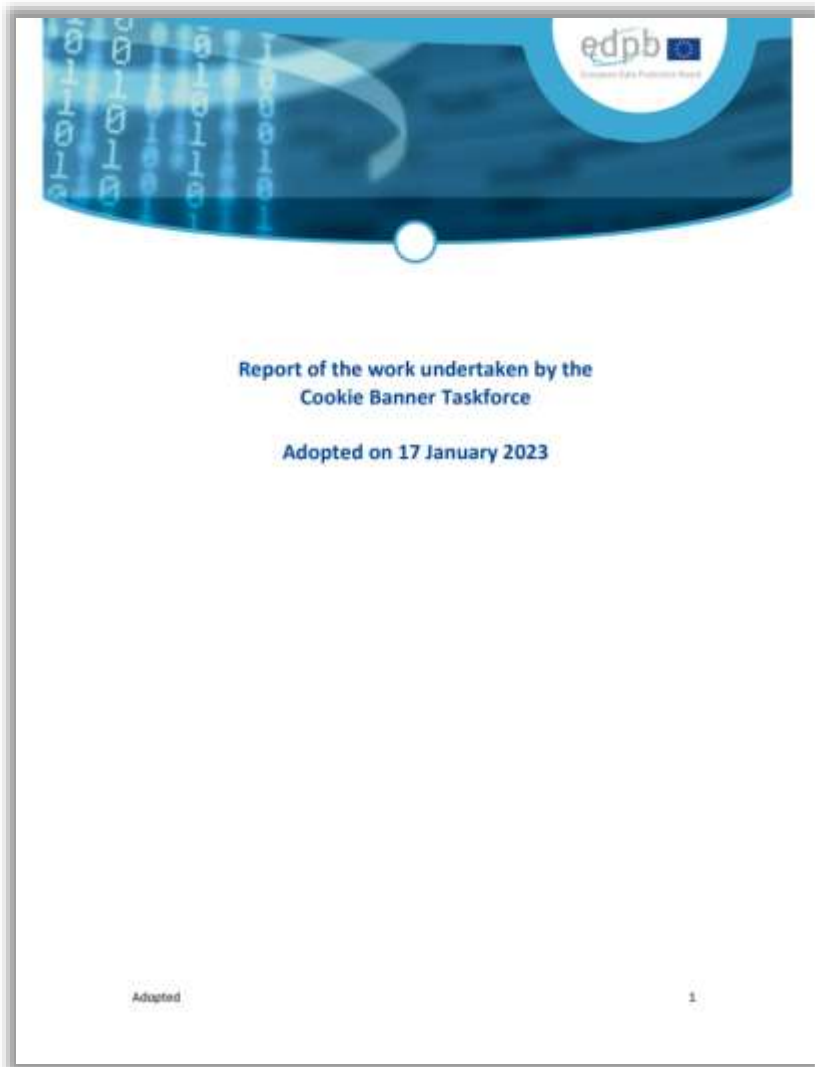
## Руководство EDPB по обработке персональных данных при предоставлении онлайн-услуг субъектам



Европейский совет по защите данных (European Data Protection Board) принял проект руководства 2/2019 по применимости ст.6(1)(b) GDPR в контексте предоставления онлайн-услуг субъектам данных.

Это руководство призвано помочь в определении правового основания обработки персональных данных в контексте заключаемых с субъектами данных контрактов на оказание им онлайн-услуг, независимо способа оплаты данных услуг. В руководстве изложены квалифицирующие признаки правомерной обработки персональных данных в соответствии со ст.6(1)(b) GDPR и рассмотрена концепция «необходимости» в том виде, в каком она применима к исполнению контракта.

## Позиция Целевой группой EDPB по практикам использования cookie-баннеров



Позиции, представленные в данном документе, являются результатом координации действий членов ЦГ EDPB с целью рассмотрения жалоб на cookie-баннеры, полученных от NOYB. Они отражают общий знаменатель, согласованный надзорными органами ЕС в их интерпретации применимых положений Директивы ePrivacy Директивы и применимых положений GDPR для анализа, который необходимо провести при рассмотрении этих жалоб. Эти позиции отражают минимальный порог в этой многоуровневой правовой системе, чтобы оценки размещения/чтения файлов cookie и последующей обработки собранных данных.

TYPE A PRACTICE – “NO REJECT BUTTON ON THE FIRST LAYER” .....	
TYPE B PRACTICE – “PRE-TICKED BOXES” .....	
TYPE C PRACTICE .....	
TYPE D & E PRACTICES : “DECEPTIVE BUTTON COLOURS” & “DECEPTIVE BUTTON CONTRAST” ..	
TYPE H PRACTICE: “LEGITIMATE INTEREST CLAIMED, LIST OF PURPOSES” .....	
TYPE I PRACTICE: “INACCURATELY CLASSIFIED « ESSENTIAL » COOKIES” .....	
TYPE K PRACTICE: “NO WITHDRAW ICON” .....	

## Тезисы руководства EDPB по обработке данных при предоставлении онлайн-услуг субъектам

- ✓ После расторжения контракта обычно несправедливо переходить на другое легальное основание (п. 41).
- ✓ Действия, связанные с контрактом после его расторжения (возврат оплаты и т.п.) тоже могут быть основаны на статье 6(1)(b). (п. 42, 44).
- ✓ Сбор детальной информации о пользователе для улучшения сервиса должен осуществляться на иных основаниях: легитимный интерес, согласие (п. 48, 49).
- ✓ Мониторинг и профилирование клиентов в целях предотвращения мошенничества выходят за рамки контракта, как основание используется легитимный интерес или правовое обязательство (п. 50).
- ✓ Обычно контракт с клиентом не является основанием для демонстрации ему таргетированной рекламы. Но если хочется, нужно учесть, что клиент имеет право возражать против прямого маркетинга по статье 21 GDPR (п. 52), учесть требования ePrivacy, мнение по WP171 и WP208 (п. 55).
- ✓ Отслеживание групп пользователей для демонстрации им определенного товара также не является необходимым для исполнения контракта (п. 56).
- ✓ Персональные данные не могут рассматриваться в качестве коммерческого товара (п. 54).
- ✓ Персонализация контента может (но не всегда) быть неотъемлемым и ожидаемым элементом некоторых онлайн-сервисов и, следовательно, может считаться необходимой для выполнения контракта с пользователем сервиса в некоторых случаях (п. 57).

Один из интересных примеров (№ 8):

Онлайн торговая площадка позволяет потенциальным покупателям просматривать и покупать товары. Торговая площадка желает показывать персонализированные предложения по продуктам, основанные на том, какие списки потенциальные покупатели ранее просматривали на платформе для повышения интерактивности. *Эта персонализация не является объективно необходимой для предоставления услуг на рынке. Таким образом, такая обработка персональных данных не может основываться на статье 6(1)(b) в качестве правового основания.*

## 295 Надлежащие принципы использования файлов cookie

Еврокомиссия 19.12.2023 опубликовала проект надлежащих принципов использования файлов cookie. Комиссия заявила, что при разработке проекта принципов залога cookie она консультировалась с Европейским советом по защите данных (EDPB), а окончательный вариант принципов будет представлен в апреле 2024 года. EDPB подчеркнул, что соблюдение организациями принципов не равнозначно соблюдению ими GDPR или Директивы ePrivacy, и что органы по защите данных остаются компетентными для осуществления своих полномочий в случае необходимости.

В проекте принципов зафиксировано, что:

- ◇ запросы на согласие не должны содержать информацию о так называемых технически необходимых файлах cookie, а также ссылки на собираемые данные, основанные на законных интересах;
- ◇ если контент сайта/приложения хотя бы частично финансируется за счет рекламы, это должно объясняться заранее, когда пользователи впервые заходят на сайт/приложение;
- ◇ цели и сценарии использования cookie должны быть описаны в краткой, ясной и легкой для выбора форме, включая четкое объяснение последствий принятия или непринятия cookie;
- ◇ в тех случаях, когда предполагается реклама на основе отслеживания или платный доступ, у пользователей должен быть дополнительный выбор менее навязчивой формы рекламы;
- ◇ согласие на использование cookies в рекламных целях не должно быть необходимым для каждого отдельного трекера, а более подробная информация о типах cookies, используемых в рекламных целях, должна предоставляться на втором уровне, с возможностью более гибкого выбора;
- ◇ не должно требоваться отдельного согласия на cookies, используемых для управления моделью показа рекламы, выбранной пользователем;
- ◇ пользователей не следует вновь просить предоставить согласие на использование файлов cookie в течение года с момента последнего запроса такого согласия, а файлы cookie должны фиксировать отказ потребителя;
- ◇ владельцам сайтов/приложений необходимо фиксировать уведомления от специализированного ПО, предоставляющего пользователям возможность заранее зафиксировать свои предпочтения в отношении файлов cookie.

The screenshot shows the website of the Information Commissioner's Office (ICO). The header includes the ICO logo and the text: "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." Below the header is a navigation menu with links: Home, Your data matters, For organisations, Make a complaint, Action we've taken, and About the ICO. The main content area is titled "Guidance on the use of cookies and similar technologies" and includes a search bar, a "Share" button, and "Download options". The page content is organized into sections: "About this guidance" with sub-questions like "What are cookies and similar technologies?", "What are the rules on cookies and similar technologies?", "How do the cookie rules relate to the GDPR?", "How do we comply with the cookie rules?", and "What else do we need to consider?". A "Contents" section lists the following topics:

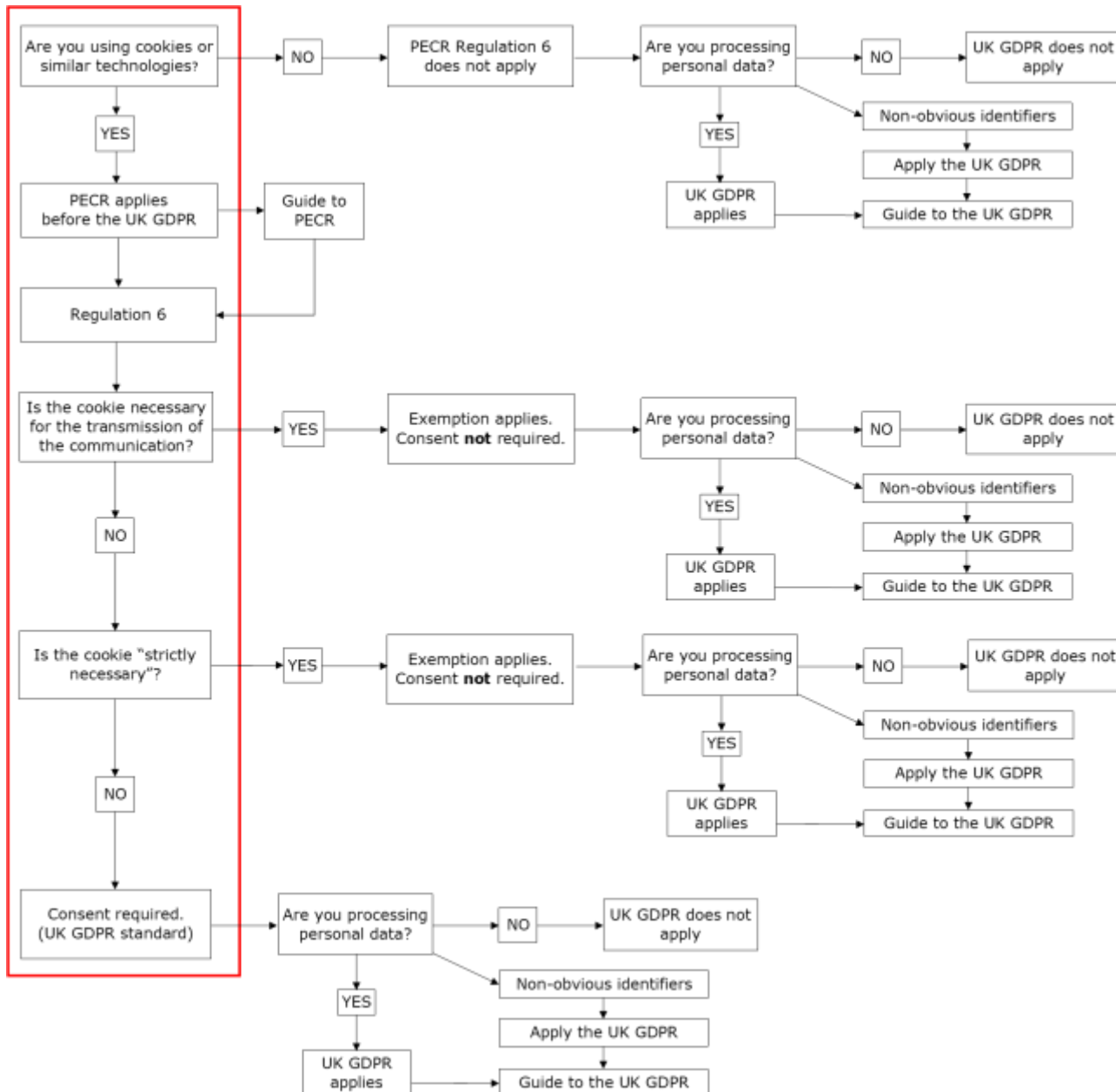
- What are cookies and similar technologies?
  - What are 'cookies'?
  - How are cookies used?
  - What are 'session' and 'persistent' cookies?
  - What are 'first party' and 'third party' cookies?
  - What are 'similar technologies'?
- What are the rules on cookies and similar technologies?
  - What does PECR say about cookies and similar technologies?
  - Who are 'subscribers' and 'users'?
  - What is 'terminal equipment'?
  - What does 'clear and comprehensive information' mean?
  - What does 'consent' mean?
  - Who do we need consent from?
  - Are we required to provide information and obtain consent for all cookies?

Британский надзорный орган Information Commissioner's Office (ICO) опубликовал руководство по использованию файлов cookie и аналогичных технологий (Guidance on the use of cookies and similar technologies), основанное на нормах «Правил конфиденциальности и электронных коммуникаций» (Privacy and Electronic Communications Regulations - PECR), которые охватывают использование файлов cookie и аналогичных технологий для хранения информации и доступа к хранимой информации на оборудовании пользователя, таком как компьютер или мобильное устройство.

PECR имеет приоритет над британским «Законом о защите данных» 2018 года (DPA) и GDPR. В то же время, PECR опирается на понятийный аппарат и общие принципы регулирования обработки и защиты персональных данных, зафиксированные в вышеуказанных правовых актах.



## 297 Руководство ICO о необходимости согласий для cookies





**AUTORITEIT  
PERSOONSGEGEVENS**

Home Actueel Over privacy ▾ Onderwerpen ▾ Zelf doen ▾ Publicaties ▾

# Websites moeten toegankelijk blijven bij weigeren tracking cookies

Nieuwsbericht / 7 maart 2019 Categorie: Cookies

Websites die bezoekers alleen toegang geven op hun site als deze akkoord gaan met het plaatsen van zogeheten 'tracking cookies' of andere vergelijkbare manieren van volgen en vastleggen van gedrag door middel van software of andere digitale methodes, voldoen niet aan de Algemene verordening gegevensbescherming (AVG). Deze normuitleg heeft de Autoriteit Persoonsgegevens vandaag gepubliceerd. De AP kreeg tientallen klachten van websitebezoekers die na het weigeren van tracking cookies geen toegang kregen tot de webpagina's die ze wilden raadplegen. De AP zal daarom de controle op de juiste naleving intensiveren en heeft inmiddels een aantal specifieke partijen hierover een brief gestuurd.

Нидерландский надзорный орган Autoriteit Persoonsgegevens (AP) в марте 2019 года руководство по использованию файлов cookie, согласно которому «стены файлов cookie» (cookie walls) нарушают требования GDPR. Стена файлов cookie - это всплывающее окно на веб-сайте, которое блокирует доступ пользователя к веб-сайту до тех пор, пока он не даст согласие на использование файлов cookie для отслеживания его действий или использования аналогичных технологий.

Согласно действующему голландскому закону о файлах cookie, функциональные и аналитические файлы cookie могут использоваться без согласия пользователя. Файлы cookie для отслеживания, подобные тем, которые используются для рекламы, могут использоваться только с согласия пользователя.

Пользователям, которые решили не давать согласие на использование файлов cookie для отслеживания их действий, все равно должен быть предоставлен доступ к веб-сайту (например, в обмен на оплату).

## Руководство CNIL по использованию файлов cookie и иных аналогичных технологий



Figure 1 - Le détail des finalités est disponible sous un bouton de déroulement que l'utilisateur peut activer sur le premier niveau d'information.



Figure 2 - Le détail des finalités est disponible en cliquant sur un lien hypertexte présent sur le premier niveau d'information

Французский надзорный орган 17.09.2020 года принял новую редакцию руководства по использованию файлов cookie, согласно которому:

- стелы файлов cookie прямо не запрещены, но законность их применения должна оцениваться в индивидуальном порядке;
- владельцы веб-сайтов должны четко информировать пользователей о целях использования файлов cookie, таких как персонализированная реклама или обмен информацией с платформами социальных сетей, а также о личности контролёров, использующих файлы cookie;
- прокрутка вниз или пролистывание веб-сайта или приложения не может рассматриваться как действительное выражение согласия на использование файлов cookie, поскольку согласие должно включать четкие позитивные действия от имени пользователей;
- отказ от использования файлов cookie должен быть таким же простым, как и принятие их, и пользователи не должны подвергаться сложным процедурам отказа;
- пользователи должны иметь возможность отозвать свое согласие на использование файлов cookie в любое время;
- файлы cookie, на которые не требуется согласие, могут использоваться для аутентификации пользователей или для сохранения содержимого корзины покупок;
- владелец сайта и третьи лица, отслеживающие действия пользователей, должны иметь возможность доказать факт получения пользовательского согласия.



Французский орган по защите данных ("CNIL") опубликовал 16.05.2022 руководство с изложением критериев для оценки законности «куки-стен» (cookie walls), т.е. практики обуславливания доступа к услуге согласием интернет-пользователя на размещение куки или аналогичных технологий отслеживания на его пользовательском устройстве. CNIL следует решению Государственного совета от 19.06.2020, который постановил, что CNIL не может наложить полный запрет на использование cookie walls.

Были определены следующие критерии:

1. Наличие реальной и справедливой альтернативы контенту или сервисам с «куки-стенами», при этом предложение платной альтернативы (т.е. требующей либо принятия cookies, либо вознаграждения за предоставленные услуги) на практике не запрещено. Однако CNIL подчеркнул, что цена должна быть разумной, то есть не настолько высокой, чтобы лишить пользователей реального выбора.
2. Ограничение целей использования cookie wall, которые должны быть направлены на получение справедливого вознаграждения за предлагаемую услугу.

## Руководство датского Datatilsynet по обработке персональных данных пользователей веб-сайтов



Датский надзорный орган в сфере персональных данных (Datatilsynet) 17.02.2019 свои рекомендации по обработке персональных данных пользователей веб-сайтов.

### Eksempel 11

Vi vil gerne registrere og opbevare personoplysninger dine seneste besøg på vores hjemmeside, og om hvordan du færdes på de forskellige dele af vores hjemmeside, til analyseformål for at forstå, hvordan forskellige mennesker bruger vores hjemmeside, så vi kan gøre det mere intuitivt. Ved at trykke her kan du sige nej tak til denne behandling.

**Tillad**

[Læs mere om vores behandling af personoplysninger.](#)

En mekanisme eller løsning til indhentning af samtykke, hvor muligheden for at afstå fra at give samtykke til behandling af personoplysninger ikke har samme meddelelseseffekt, som muligheden for at give samtykke, vil ikke være lovlig, idet den registrerede indirekte skubbes i retning af at give samtykke.

Det er efter Datatilsynets opfattelse i strid med det grundlæggende princip om gennemsigtighed.

Vi vil gerne registrere og opbevare personoplysninger dine seneste besøg på vores hjemmeside, og om hvordan du færdes på de forskellige dele af vores hjemmeside, til analyseformål for at forstå, hvordan forskellige mennesker bruger vores hjemmeside, så vi kan gøre det mere intuitivt. [Læs mere om vores behandling af personoplysninger.](#)

**Tillad**

**Afslå**

Her har de to valg mellem at give samtykke eller ikke at give det samme meddelelseseffekt, og valget er dermed gennemsigtigt for den registrerede.

## 302 Рекомендации датского Datatilsynet по использованию cookie walls

 DATATILSYNET

### Brug af cookie walls

Dato: 20-02-2023

Nyhed

Datatilsynet har truffet to principielle afgørelser vedrørende brug af såkaldte cookie walls på hjemmesider og udgiver i den forbindelse også et sæt generelle retningslinjer for brugen af sådanne samtykkeløsninger.



Siden Datatilsynet i begyndelsen af 2020 satte fokus på behandling af personoplysninger om hjemmesidebesøgende, har tilsynet modtaget en række henvendelser om brugen af såkaldte cookie walls.

Датский орган по защите данных ("Datatilsynet") 20.02.2023 опубликовал общие рекомендации по использованию т.н. "стен cookie" (cookie walls). Руководство включает четыре критерия, которые станут отправной точкой для оценки Datatilsynet того, соответствует ли использование стены cookie в конкретном случае GDPR.

### 303 Датский Datatilsynet критикует подход сайта www.eb.dk к согласию на cookies

Датский надзорный орган в сфере персональных данных (Datatilsynet) 09.11.2022 выступил с серьезной критикой решения о согласии, используемого JP/Politiken на сайте www.eb.dk, поскольку согласие посетителей сайта не было достаточно информированным.

Посетителям сайта предлагались три варианта согласия на cookies – «Только необходимое», «Настроить параметры» и «Принять все». На "первом уровне" решения о согласии указывалось, что JP/Politiken обрабатывает персональные данные в статистических и маркетинговых целях. На "втором уровне", доступ к которому посетитель мог получить, нажав на кнопку «Настроить параметры», посетитель мог дать отдельные согласия на обработку в целях персонализации, статистики и маркетинга.

Надзорный орган решил, что посетители сайта www.eb.dk не дали информированного согласия, поскольку посетители, нажавшие на кнопку «Принять все», не получили информацию обо всех целях обработки - так как информация о всех целях обработки появилась только во "втором уровне" согласия.

*Обновленная версия согласия сайта www.eb.dk на cookies.*

Powered by **Cookiebot** by Usercentrics

**Samtykke**    Detaljer    Annonceindstillinger    Om

**Det er dit valg**

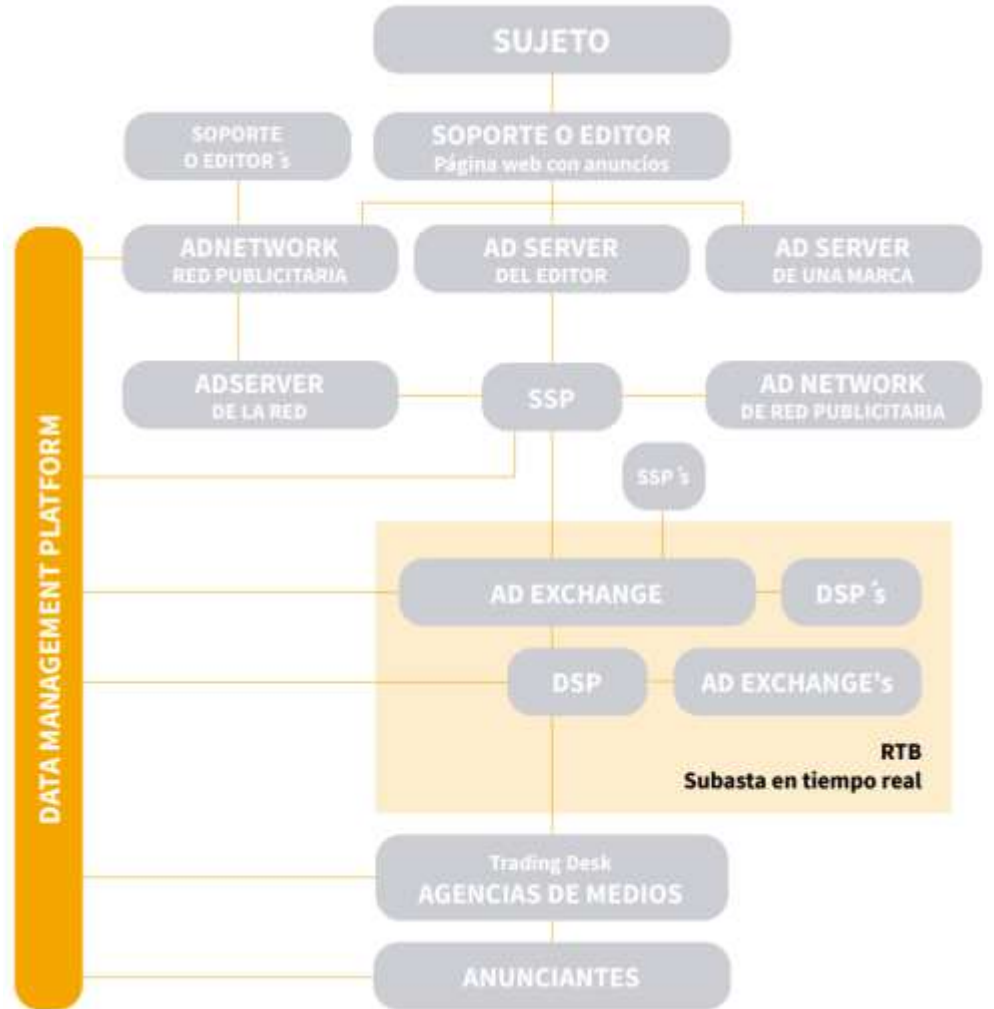
Vi ønsker dit samtykke til at anvende cookies og indsamle persondata om IP-adresse, ID og din browser til præferencer, statistik og marketingformål. Disse oplysninger videregives til vores **samarbejdspartnere**, der opbevarer og tilgår oplysninger på din enhed for at vise dig målrettede annoncer, levere tilpasset indhold, foretage annonce- og indholdsmåling, lave produktudvikling og opnå målgruppeindsigt. Se mere information under **indstillinger** og i vores **persondatapolitik**.

Du kan altid trække dit samtykke tilbage eller ændre indstillinger fra vores "Cookieindstillinger". Dit valg anvendes på

<b>Nødvendig</b> <input type="checkbox"/>	<b>Præferencer</b> <input checked="" type="checkbox"/>	<b>Statistik</b> <input checked="" type="checkbox"/>	<b>Marketing</b> <input checked="" type="checkbox"/>
--	---	---	---

**Kun nødvendige**    **Tillad valgte**    **Tillad alle**

## 304 Руководство испанского AEPD по использованию файлов cookie





## Guidance Note: Cookies and other tracking technologies

April 2020



The DPC's regulatory role in relation to cookies and tracking technologies .....	
The ePrivacy Regulations .....	
What are cookies? .....	
What other types of tracking technologies are in use? .....	
What is terminal equipment? .....	
What is the law on cookies and what is its purpose? .....	
Consent .....	
Which cookies are exempt from the requirement to obtain consent from the user or subscriber? .....	
Do analytics cookies require consent? .....	
Can you obtain consent for multiple purposes at the same time? .....	
Withdrawal of consent.....	
How do you obtain consent in practice? .....	
Can you use implied consent for the use of cookies and tracking technologies? .....	
Clear and comprehensive information .....	
Transparency information and responsibilities under the GDPR .....	
Pre-checked boxes and sliders.....	
Requirements for the use of consent management providers (CMPs) .....	
Requirements for cookie banners.....	
Can you rely on the user's browser settings to infer consent? .....	
Confusing interfaces .....	
Cookie lifespans .....	
Joint controllers .....	
Processing of personal data .....	
Do you need to conduct a data protection impact assessment (DPIA)? .....	
Special category data.....	
Location tracking or derivation of location information from cookies.....	
Compliance .....	

# Руководство CPDP по использованию файлов cookie и иных аналогичных технологий



## Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021 [9677876]

VEDI ANCHE

- [Allegato 1 - Scheda di sintesi](#)

- [Comunicato stampa del 10 luglio 2021](#)

- [Pagina tematica COOKIE](#)



[doc. web n. 9677876]

Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021  
(Pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021)

Registro dei provvedimenti  
n. 231 del 10 giugno 2021

### IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stazione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il dott. Fabio Mattei, segretario generale;

VISTA la direttiva 2002/21/CE del 7 marzo 2002, del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (c.d. direttiva quadro), come successivamente modificata e integrata;

VISTA la direttiva 2002/58/CE del 12 luglio 2002, del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. direttiva ePrivacy), come modificata dalla direttiva 2009/136/CE del 25 novembre 2009, del Parlamento europeo e del Consiglio;

VISTO il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), come



Allegato n. 1 al provvedimento del Garante per la protezione dei dati personali n. 231 del 10 giugno 2021 "Linee guida cookie e altri strumenti di tracciamento"

## LINEE GUIDA COOKIE E ALTRI STRUMENTI DI TRACCIAMENTO

### SCHEDA DI SINTESI

Oggetto	Cookie e altri strumenti di tracciamento.
Normativa	Artt. 122 del Codice e 4, punto 11), 7, 12, 13 e 25 del Regolamento.
Cookie ed altri strumenti di tracciamento	I cookie sono di regola stringhe di testo che i siti web (cd. publisher o "prima parte") visitati dall'utente ovvero siti o web server diversi (cd. "terze parti") posizionano e archiviano all'interno di un dispositivo terminale nella disponibilità dell'utente (cd. identificatori "attivi"). Analoghe funzioni possono essere svolte da altri strumenti che, pur utilizzando una tecnologia diversa (c.d. identificatori "passivi"), consentono di effettuare trattamenti analoghi a quelli svolti per il tramite dei cookie.
Cookie ed altri identificatori tecnici	Sono utilizzati al solo fine di "effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'utente o dall'utente a erogare tale servizio" (cf. art. 122, comma 1 del Codice). Non richiedono l'acquisizione del consenso, ma vanno indicati nell'informativa.
Cookie analytics prime e terze parti	Sono equiparabili ai cookie e agli altri identificatori tecnici solo se: <ul style="list-style-type: none"> <li>- vengono utilizzati unicamente per produrre statistiche aggregate e in relazione ad un singolo sito o una sola applicazione mobile;</li> <li>- viene mascherata, per quelli di terze parti, almeno la quarta componente dell'indirizzo IP;</li> <li>- le terze parti si astengono dal combinare i cookie analytics, così minimizzati, con altre elaborazioni (file dei clienti o statistiche di visite ad altri siti, ad esempio) o dal trasmetterli ad ulteriori terzi. È tuttavia consentita alle terze parti la produzione di statistiche con dati relativi a più domini, siti web o app che siano riconducibili al medesimo publisher o gruppo imprenditoriale.</li> </ul> Il titolare che effettui in proprio la mera elaborazione statistica dei dati relativi a più domini, siti web o app ad esso riconducibili può utilizzare anche i dati in chiaro, nel rispetto del vincolo di finalità.
Cookie e altri identificatori di tracciamento con funzione non tecnica	Utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (pattern) al fine del raggruppamento dei diversi profili all'interno di cluster omogenei di diversa ampiezza, in modo che sia possibile anche modulare la fornitura del servizio in modo sempre più personalizzato, nonché inviare messaggi pubblicitari mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete.
Principali novità introdotte dal GDPR aventi effetti sull'uso dei cookie e altri strumenti di tracciamento	<ul style="list-style-type: none"> <li>- accountability;</li> <li>- integrazione dell'informativa (specificare anche i tempi di conservazione dei dati);</li> <li>- rafforzamento del consenso (deve essere "inequivocabile");</li> <li>- rispetto dei principi di privacy by design e by default.</li> </ul>

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876>

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9679270>

<https://iabeurope.eu/blog/whats-in-the-latest-cookie-guidance-from-italys-garante/>


## 307 Решение датского Datatilsynet по использованию стены из cookie-файлов

Датский орган по защите данных ("Datatilsynet") 20.02.2023 принял решение, в котором он признал использование компанией 'cookie-walls' в нарушение ст.6(1)(a) GDPR и обязал компанию продемонстрировать, что обработка персональных данных осуществлялась в статистических целях в соответствии со статьей 6(1)(a) GDPR, со ссылкой на статьи 4(11), 5(1)(a) и 5(2), после подачи жалобы.

Веб-сайт компании Jysk Fynske Medier P/S позволял посетителям получить доступ к части контента сайта, дав согласие на обработку персональных данных, или ко всему контенту сайта, подписавшись на его услуги. В целом механизм, при котором посетители сайта могут получить доступ к содержанию сайта или услуги в обмен либо на согласие на обработку персональных данных, либо на оплату, соответствует требованиям к действительному согласию в соответствии с правилами защиты данных.

Однако особый подход компании, заключающийся в предоставлении частичного доступа к контенту после получения согласия посетителей, в то время как предоставление доступа ко всему контенту при подписке посетителей, не соответствует требованиям действительного согласия в соответствии с GDPR. В этой связи Datatilsynet пояснил, что это произошло потому, что услуга, предлагаемая на основании согласия, в значительной степени не была эквивалентна той, которая предлагалась на основании подписки и оплаты, что означает, что посетителям не был представлен свободный выбор. Кроме того, компания не доказала, что обработка персональных данных в статистических целях была необходима в связи с получением согласия от посетителей. Следовательно, Datatilsynet установил, что компания не соблюдает требование добровольности согласия в соответствии с GDPR, и что обработка статистических данных в соответствии со статьей 6(1)(a) GDPR является незаконной.

## Руководство LfDI Baden-Württemberg по использованию файлов cookie и иных аналогичных технологий



FAQ  
Cookies und Tracking  
durch Betreiber von Webseiten und  
Hersteller von Smartphone-Apps

Der Landesbeauftragte für  
Datenschutz und  
Informationsfreiheit  
Baden-Württemberg

Wir glauben, dass Ihre Daten Ihr Eigentum sind und unterstützen Ihr  
Recht auf Privatsphäre und Transparenz.

Wählen Sie eine Datenzugriffsebene und -dauer aus, um auszuwählen, wie wir Ihre Daten verwenden und weitergeben.

SILBER
  GOLD
  PLATIN
 3 Monate ▾

Höchste Privatsphäre. Datenzugriff nur für notwendige Website-Operationen. Die Daten werden an Dritte weitergegeben, um sicherzustellen, dass die Website sicher ist und auf Ihrem Gerät funktioniert

Einstellungen Speichern

Wir benötigen Ihre Einwilligung, um fortzufahren.

Um unsere Webseite für Sie optimal gestalten und verbessern zu können, verwenden wir Cookies.

Weitere Informationen zu Cookies erhalten Sie in unserer [Datenschutzerklärung](#).

- Technisch notwendige Cookies
- Drittanbieter-Cookies (Social-Media-Elemente von Facebook, Twitter und Google werden auf der gesamten Webseite aktiviert.)

Alle Akzeptieren

Akzeptieren



# Check-list cookies<sup>1</sup>

L'énumération des obligations dans la présente check-list n'est **pas exhaustive**. Le présent document est un **simple outil** grâce auquel l'Autorité de protection des données souhaite encourager l'utilisation correcte des cookies. Les éléments qui y sont repris ne peuvent dès lors pas être considérés comme de nouvelles obligations.



## Consentement préalable

- Je ne dépose (ni ne me procure accès à) aucun cookie qui ne soit pas strictement nécessaire avant d'avoir obtenu le consentement valable à cet effet :



## Consentement libre

- Je n'utilise pas de "cookie walls";
- Je ne prévois pas de bouton "accepter tous les cookies" (ou similaire) sans prévoir au même "niveau" un bouton "refuser tous les cookies non essentiels" (ou similaire);
- Je n'utilise pas de techniques pouvant être qualifiées de "déceptive design"<sup>2</sup> (par ex. l'incitation par l'utilisation de la couleur);



## Quand ne faut-il pas de consentement ?



- J'ai contrôlé la catégorisation des "cookies techniques essentiels"<sup>3</sup> (tels que ceux pour le load balancing) ;
- J'ai contrôlé la catégorisation des "cookies fonctionnels strictement nécessaires"<sup>4</sup> (tels que les cookies pour la conservation temporaire du choix de la langue, les préférences en matière de cookies ou le contenu du panier). Ceci inclut **uniquement** les cookies qui sont strictement nécessaires pour fournir un service<sup>5</sup> explicitement demandé par le "visiteur" ;
- J'ai veillé à ce qu'aucun autre cookie que ceux ci-dessus ne soit placé sans l'obtention préalable du consentement valable du "visiteur".

### Notes bas de page

1 Et la présente check-list s'applique à toutes les "cookies", et ce, quel que soit le type de traitement de données qu'elles impliquent, à l'exception de celles qui sont strictement nécessaires à l'exécution d'un contrat ou à la fourniture d'un service demandé par le "visiteur".

2 L'ESPd a publié des lignes directrices sur le consentement, point 39. « Afin que le consentement soit libre, volontaire, éclairé par des services et que les données ne soit pas être conditionnées au consentement d'un utilisateur au stockage d'informations, ou à l'accès aux informations déjà stockées, un équipement terminal (le utilisateur doit être "cookie wall", consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre> ».

3 Les boutons "Paramètres" et "OK" et la fonction "Tout accepter" ne sont pas, en soi, acceptables en matière de consentement préalable par l'Autorité de protection des données, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

4 Voir aussi notre communiqué de presse, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

5 Par exemple, les boutons "Tout refuser" et "Tout accepter" sont acceptables en matière de consentement préalable par l'Autorité de protection des données, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

6 Voir aussi l'Article 65 des lignes directrices relatives au consentement, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

7 Voir aussi l'Article 65 des lignes directrices relatives au consentement, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

8 Voir aussi l'Article 65 des lignes directrices relatives au consentement, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

9 Voir aussi l'Article 65 des lignes directrices relatives au consentement, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

10 Voir aussi l'Article 65 des lignes directrices relatives au consentement, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

11 Article 102.2.2 du Règlement (UE) 2018/1725 relatif à la protection des données personnelles et à la libre circulation de ces données.

12 En particulier, pour l'Article 65 des lignes directrices relatives au consentement, voir le paragraphe 33 de l'Annexe (4) du Groupe de travail Article 29 sur la protection des données, consultable via le lien suivant : <https://www.autoriteprotectiondonnees.be/fr/actualites/2022/03/24/consentement-libre>.

13 "Where they are otherwise necessary for strictly necessary" but for website operation, they are not strictly necessary to provide a service which is strictly necessary for the user for website use. In fact, the user can access the service without the website being online or available.

14 De plus, les cookies sont strictement nécessaires à la fourniture d'un service demandé par le "visiteur" si le "visiteur" a explicitement demandé ce service.

## Руководство гамбургского HmbBfDI по соблюдению операторами веб-сайтов требований TTDSG и GDPR

◇ 21.04.2023 уполномоченный Гамбурга по защите данных и свободе информации (HmbBfDI) опубликовал руководство, призванное разъяснить основные аспекты функционирования веб-сайта и облегчить соблюдение требований по защите данных. Руководство посвящено таким темам, как согласие, дизайн баннера cookie, интеграция контента третьих лиц, информационные положения, технические аспекты и последствия несоблюдения требований.

◇ В соответствии с Федеральным законом о регулировании защиты данных и конфиденциальности в сфере телекоммуникаций и телемедиа (TTDSG) обязательство получать согласие пользователя перед размещением файлов cookie применяется независимо от того, обрабатываются ли персональные данные. Однако, поскольку использование файлов cookie часто связано с обработкой персональных данных, может возникнуть необходимость в получении дополнительного согласия в соответствии с GDPR. Оба заявления о согласии, согласно TTDSG и GDPR, могут быть получены одновременно, если соответствующая информация включена в баннер согласия.

◇ Операторы веб-сайтов в значительной степени свободны в оформлении баннеров согласия на использование файлов cookie в отношении цвета, размера или контраста, однако баннер всегда должен позволять пользователю сайта легко понять смысл сообщения. ВПервый уровень баннера согласия должен обеспечивать возможность полного согласия (т.е. кнопку "Принять все"), столь же заметную функцию отказа (т.е. кнопку "Отклонить все") и, при необходимости, возможность получения более подробной информации.

◇ Говоря о контенте третьих лиц, руководство отмечает, что при интеграции карт, видео, шрифтов, интеграции социальных сетей и других сервисов в веб-сайт, в принципе, также необходимо получить согласие в соответствии с TTDSG и, если применимо, GDPR. В руководстве отмечается, что, насколько это возможно, фактическая интеграция стороннего контента должна технически происходить, когда пользователи явно запрашивают такую услугу, например, хотят посмотреть видео.

## Руководство норвежского Datatilsynet по веб-аналитике и отслеживанию пользователей



**Datatilsynet**

### Råd for analyse og sporing på nettsted

Det finnes mange analyse- og sporingsverktøy på markedet, men det betyr ikke nødvendigvis at det er lovlig å ta dem i bruk på nettstedet ditt. Her er noen råd på veien.

Publisert: 27.07.2023

**1 Forhold deg til personvernforskriften (GDPR)**

Når du tar i bruk verktøy for analyse og sporing på nettstedet, må du være forberedt på å følge reglene i personvernforskriften (GDPR). Dette gjelder selv om du ikke kjenner navnet eller identiteten til de som besøker nettstedet ditt. Analyseverktøyene samler nemlig inn mye informasjon om de besøkende som enten alene eller i kombinasjon kan utgjøre personopplysninger.

En IP-adresse vil som regel i seg selv regnes som en personopplysning. Cookie-ID, lokasjonsdata eller detaljert informasjon om brukernes enheter kan også utgjøre personopplysninger. Ofte blir slik informasjon kombinert med informasjon om de besøkendes adferd på nettstedet, og da regnes også dette som personopplysninger.

[Les mer om personopplysninger.](#)

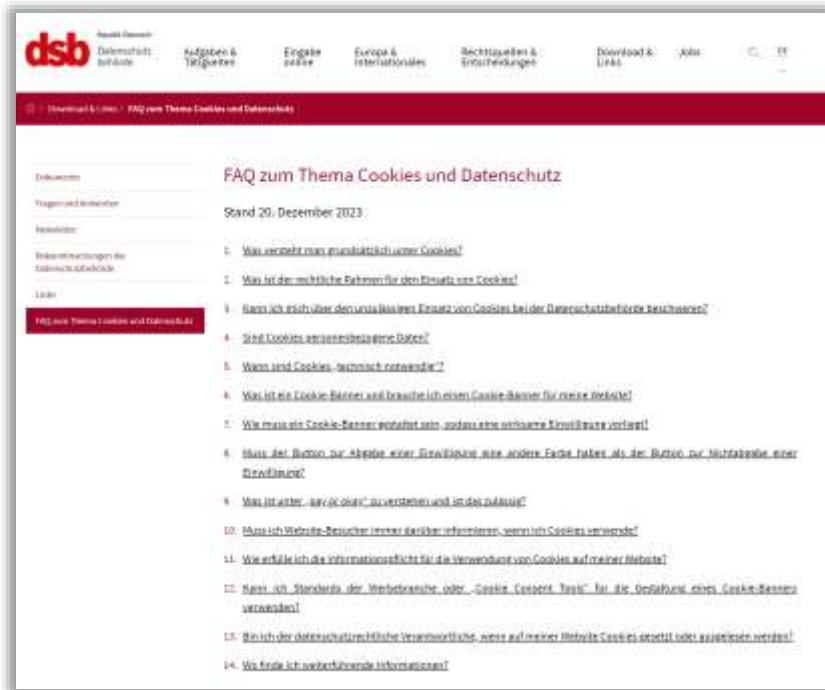
**2 Minimer datainnsamlingen**

Det er ikke lov å samle inn flere personopplysninger enn du faktisk har behov for. Dersom du i dag har et analyseverktøy som samler inn opplysninger som du ikke bruker til noe, bryter du loven. Velg et analyseverktøy som bare gir deg den informasjonen du trenger og faktisk har nytte av.

Норвежский орган по защите данных (Datatilsynet) опубликовал 27.07.2023 рекомендации по использованию по веб-аналитике и отслеживанию пользователей. Datatilsynet указал, что компании должны:

- минимизировать сбор данных;
- не полагаться на баннеры cookie, подчеркивая, что существуют разные правила размещения cookie и обработки персональных данных;
- не позволять другим лицам использовать персональные данные со своих сайтов;
- учитывать дополнительные требования, действующие при обработке чувствительных персональных данных;
- избегать передачи персональных данных в небезопасные третьи страны; предоставлять простую и понятную информацию пользователям сайта;
- уважать права пользователей веб-сайта.

## 312 FAQ австрийского DSB по использованию cookies



Австрийский орган по защите данных (DSB) 20.12.2023 опубликовал часто задаваемые вопросы (FAQ) о файлах cookie и защите данных, который содержит следующую информацию:

- значения файлов cookie и того, являются ли они персональными данными;
- правовая база для использования файлов cookie;
- обязательны ли баннеры cookie для веб-сайта;
- разъяснения по поводу технически необходимых файлов cookie;
- должна ли кнопка согласия быть другого цвета;
- В каких случаях допускается ли модель "плати или соглашайся" (pay or okay);
- как должен быть оформлен баннер cookie для эффективного согласия;
- информация для пользователей веб-сайта об использовании файлов cookie;
- можно ли использовать стандарты рекламной индустрии или инструменты для получения согласия на использование файлов cookie при разработке баннеров cookie;
- кто несет ответственность за защиту данных, если файлы cookie размещены на их сайте.



<b>Проблема</b>	<b>Позиция ICO, CNIL и AP</b>
<b>Согласие</b>	<p>Подразумеваемое согласие недостаточно - требуется явно выраженное согласие согласно требованиям GDPR</p> <p>Организации должны иметь возможность продемонстрировать получение согласия в надлежащей форме</p>
<b>Стены cookie</b>	Не признаются правомерными
<b>Технические cookies</b>	Согласие не требуется
<b>Аналитические cookies</b>	<p>ICO: согласие требуется</p> <p>CNIL: согласие не требуется при определенных условиях</p> <p>AP: согласие не требуется при определенных условиях</p>
<b>Демонстрация прозрачности</b>	Повышенные требования к информированности пользователей

## Обзор законодательства ЕС по использованию файлов cookie от DLA Piper

COUNTRY	HAS THERE BEEN RECENT ENFORCEMENT?	CAN A USER PROVIDE CONSENT VIA BROWSER SETTINGS?	ARE COOKIE WALLS ALLOWED?	CAN CONSENT BE IMPLICIT?	COUNTRY	HAS THERE BEEN RECENT ENFORCEMENT?	CAN A USER PROVIDE CONSENT VIA BROWSER SETTINGS?	ARE COOKIE WALLS ALLOWED?	CAN CONSENT BE IMPLICIT?
<a href="#">Austria</a>	No.	Unclear, but likely no.	Yes (currently).	Unclear, but likely no.	<a href="#">Ireland</a>	No.	No.	No.	No.
<a href="#">Belgium</a>	Yes - 1 fine.	No.	No.	No.	<a href="#">Latvia</a>	No.	No.	No.	No.
<a href="#">Bulgaria</a>	No.	Unclear - no specific rules or guidance.	No.	No.	<a href="#">Lithuania</a>	No.	Unclear, although it is unlikely (see guidance).	No.	No.
<a href="#">Croatia</a>	No.	No.	Unclear.	No; however, see additional guidance for exceptions.	<a href="#">Luxembourg</a>	No.	Yes.	No.	No (see additional guidance for exceptions).
<a href="#">Cyprus</a>	No.	No.	No.	No.	<a href="#">Malta</a>	No.	Unclear.	Unclear.	Unclear.
<a href="#">Czech Republic</a>	No.	Yes; however, see additional guidance for details.	No.	Yes; however, see additional guidance for details.	<a href="#">Netherlands</a>	Yes.	No.	No.	No.
<a href="#">Denmark</a>	No.	No.	No.	No.	<a href="#">Norway</a>	No.	No.	No.	No.
<a href="#">Estonia</a>	No.	No.	No.	No.	<a href="#">Poland</a>	No.	Yes.	Unclear; however, unlikely (see additional guidance).	No.
<a href="#">Finland</a>	Yes - 1 case.	No.	Unclear, although it is unlikely (see additional guidance).	No.	<a href="#">Portugal</a>	No.	No.	No.	No.
<a href="#">France</a>	Yes - 3 fines, 3 court cases.	No.	Unclear, assessed on a case-by-case basis (see additional guidance).	No.	<a href="#">Romania</a>	No.	Yes.	Unclear (see additional guidance).	No.
<a href="#">Germany</a>	Yes - 1 case.	No.	Unclear (see additional guidance)	Unclear (see additional guidance)	<a href="#">Slovak Republic</a>	No.	Yes.	No.	Yes.
<a href="#">Hungary</a>	No.	No.	No.	No.	<a href="#">Slovenia</a>	No.	Unclear (see additional guidance).	No.	No.
<a href="#">Italy</a>	No.	Yes.	Unclear; however, unlikely (see additional guidance).	Yes.	<a href="#">Spain</a>	Yes, 41 fines on non-compliance since 2014.	Yes; however, see additional guidance for details on limitations.	Unclear (see additional guidance).	Yes.
					<a href="#">Switzerland</a>	No.	Yes.	Unclear (see additional guidance).	Yes.
					<a href="#">UK</a>	No.	No.	No.	No.

## 315 Руководство немецкого BfDI по защите данных и телекоммуникациях



В руководстве подробно описаны юридические и технические вопросы, касающиеся защиты данных в сфере телекоммуникаций. Кроме того, оно содержит обзор регулирующего законодательства, включая GDPR и Федеральный закон о регулировании защиты данных и конфиденциальности в сфере телекоммуникаций и телемедиа от 23.06.2021 года (TTDSG).

[https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2023/12\\_Info5-Neuaufgabe.html?nn=251928](https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2023/12_Info5-Neuaufgabe.html?nn=251928)

<https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO5.html?nn=251928>

## 316 Кипрский комиссар о результатах аудита использования файлов cookie



Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα  
Ανεξάρτητη εποπτική αρχή για την προστασία του ατόμου

Πληροφορίες για πολίτες Πληροφορίες για οργανισμούς Νομοθεσία Θεσμικές Ενότητες Διεθνής Συνεργασία Γραφείο Επιτρόπου

Αρχείο Έκθεσης Γραφείο Επιτρόπου Γ.Π.Α. / Ανακοίνωση Του Ελέγχου Για Τη Χρήση Cookies Από Ιστοσελίδες

### Αποτελέσματα των ελέγχων για τη χρήση Cookies από ιστοσελίδες

**Ανακοίνωση**  
Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα  
σε σχέση με τα αποτελέσματα των ελέγχων  
για τη χρήση Cookies από ιστοσελίδες

Σε συνέχεια των προηγούμενων Ανακοινώσεων μου σε σχέση με τους ελέγχους που διενεργώ το Γραφείο μου σε ιστοσελίδες σχετικά με τη χρήση cookies, ενημερώνω ότι έχουν ολοκληρωθεί περί των 30 ελέγχων που αφορούν κυρίως σε εδημοσιογραφικές και άλλες συναφείς ιστοσελίδες ενημέρωσης του κοινού.

Υπενθυμίζεται ότι τα cookies είναι μικρά αρχεία δεδομένων που αποθηκεύονται από έναν δικτυακό τόπο στον υπολογιστή ή στη φορητή συσκευή του επισκέπτη, για τα οποία με βάση τη νομοθεσία απαιτείται η λήψη συγκατάθεσης των χρηστών. (με εξαίρεση αυτά που είναι απολύτως αναγκαία για να μπορεί ο παραχás υπηρεσίας της κοινότητας της πληροφορίας να παρέχει την υπηρεσία των οποία έχει ζητήσει ρητά ο χρήστης).

Οι διαχωριστές των ιστοσελίδων στις οποίες διενεργήθηκε έλεγχος είχαν λάβει επικοινωνία με τα ευρήματα του ελέγχου, τα οποία κλήθηκαν να διορθώσουν. Λόγω του ότι οι συγκεκριμένα έλεγχοι ήταν οι πρώτοι του είδους, και οι διαδικτυακοί τόποι αναβαθμίζονται συνεχώς με την χρήση νέων τεχνολογιών, είχε δοθεί στους διαχωριστές των ιστοσελίδων μεγάλο χρονικό περιθώριο συμμόρφωσης και αποστέλλαν σφαιρικά επιστολές με υποδείξεις / διευκρινήσεις σχετικά με προβλήματα που είχαν παρουσιαστεί κατά τους ελέγχους.

Τα κυριότερα θέματα που είχαν διαπιστωθεί κατά τους ελέγχους είναι τα ακόλουθα:

1. Στις περισσότερες ιστοσελίδες δεν υπήρχε ενημέρωση σχετικά με τους σκοπούς χρήσης των cookies.
2. Ιστοσελίδες οι οποίες είχαν ενημέρωση για την χρήση cookies, δεν λάμβαναν την ρητή συγκατάθεση των χρηστών για την χρήση cookies, ή ο τρόπος λήψης της συγκατάθεσης δεν πληρούσε τις προϋποθέσεις για νόμιμη συγκατάθεση (ελεύθερη, με δυνατότητα ανάκλησης, κλπ).
3. Κάποια cookies όπως π.χ. για μέτρηση της επισκεψιμότητας της ιστοσελίδας ήταν λανθασμένα κατηγοριοποιμένα ως «απολύτως αναγκαία».

Μετά από τις υποδείξεις μας έχουμε διαπιστώσει ότι υπήρξε συμμόρφωση με τις πρόνοιες της νομοθεσίας και της στόχευσης του ελέγχου. Οι έλεγχοι πραγματοποιήθηκαν εντός συγκεκριμένου χρονικού διαστήματος, και θα σκανελλεχτεί η συμμόρφωση των ιστοσελίδων.

Στο ερώτημα που τίθεται συνήθως, πως αντιμετωπίζουν την χρήση των cookies άλλες Εποπτικές Αρχές, θα ήθελα να αναφέρω ότι έχουν δεχθεί και διεξάγουν αντίστοιχους ελέγχους και προβαίνουν σε διάφορες ενέργειες με στόχο την συμμόρφωση με την νομοθεσία.

Το Γραφείο μου παρακολουθεί και συμμετέχει στις συζητήσεις των ομάδων του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ) που εξετάζουν διάφορα θέματα σε σχέση με την χρήση cookies, για περαιτέρω ομοιομορφία στην προσέγγιση των μέλών του ΕΣΠΔ. Αν παρ'αυτά ανόγκη θα προβούμε σε επιπρόσθετους ελέγχους για τα θέματα που είναι υπό-αυτίτητες, όπως π.χ. σε σχέση με την χρήση των εργαλείων Google Analytics και Facebook connect / pixel αλλά και άλλων νέων τεχνολογιών.

Управление уполномоченного по защите персональных данных в Республике Кипр опубликовало 08.05.2023 отчет о проведенном им аудите использования файлов cookie на 30 новостных и других информационных сайтах. Основные нарушения, обнаруженные в ходе аудита:

- отсутствовала информация о целях использования файлов cookie;
- веб-сайты, на которых была информация об использовании cookie, не получали прямого согласия пользователей на использование cookie, или их метод получения согласия не соответствовал условиям законного согласия;
- некоторые файлы cookie, например, используемые для измерения посещаемости сайта, были неверно отнесены к категории "абсолютно необходимых".

## 317 Инструмент EDPB по аудиту веб-сайтов для проверки соответствия требованиям

EDPB > EDPB Website Auditing Tool > Releases

Our Support Team will be operating at a reduced capacity from Wednesday (31 January) to Friday (2 February) incl. During this period, our team may experience limitations in handling all support requests promptly.

Released date ▾ ⌵

### EDPB Website Auditing Tool

#### Assets 7

- Source code (zip) [↓](#)
- Source code (tar.gz) [↓](#)
- Source code (tar.bz2) [↓](#)
- Source code (tar) [↓](#)

#### Other

- Linux [↗](#)
- Mac OS [↗](#)
- Windows [↗](#)

#### Evidence collection

1.1.2-evidences-277.json [↗](#) 6833196f [↗](#)

Collected 6 days ago

SHA256(website-audit\_1.1.2\_amd64.deb) = f50b2b28fdd0f6d1041d4921b372ae7aa184b93da5d6466f4a69e31ed74fcff5

SHA256(website-audit Setup 1.1.2.exe) = f00bec0ace8baf1b20b674456c5980eee5f7e291dd6009a31af417798a19fb71

SHA256(website-audit-1.1.2-universal.dmg) = 0d68b6bf5de87ccdfab07ae61720f11e75d7e671ac3a6990ec5081164a496dcf

[↗ 7c7fa097](#) [↗ 1.1.2](#) Released 6 days ago by [↗](#)

## 318 Решение немецкого DSK по оценке моделей чистой подписки на веб-сайтах

Немецкая конференция по защите данных ("DSK") опубликовала свое решение, принятое 22.03.2023 года, относительно оценки моделей чистой подписки на веб-сайтах. В принципе отслеживание поведения пользователей может быть основано на согласии, если в качестве альтернативы предлагается модель без отслеживания, даже если она платная. Однако услуга, которую пользователи получают в рамках платной модели, должна, во-первых, представлять собой эквивалентную альтернативу услуге, которую они могут получить после предоставления согласия; и, во-вторых, согласие должно отвечать всем требованиям GDPR, в частности, должны быть выполнены требования статей 4(11) и 7 GDPR.

Вопрос о том, может ли вариант оплаты (например, ежемесячная подписка) рассматриваться как эквивалентная альтернатива согласию на отслеживание, зависит, в частности, от того, предоставляется ли пользователю эквивалентный доступ к той же услуге за плату, которая является обычной на рынке. Как правило, доступ может считаться эквивалентным, если предложения включают, по крайней мере, в основном одну и ту же услугу.

Когда пользователи подписываются на опцию "без отслеживания" и не дают дополнительного согласия, в соответствии со статьей 25(1) Федерального закона о регулировании защиты данных и конфиденциальности в телекоммуникациях и телемедиа от 23 июня 2021 года ("TTDSG"), хранение информации в терминальном оборудовании пользователей и доступ к уже хранящейся в нем информации может осуществляться только в том случае, если это абсолютно необходимо для предоставления услуги информационного общества, явно запрошенной абонентом или пользователем.

Эффективность деклараций о согласии лиц, не являющихся абонентами, должна быть обеспечена для так называемых моделей чистой подписки. При наличии нескольких целей обработки, которые существенно отличаются друг от друга, согласие должно быть гранулированным, указав, среди прочего, что общее согласие для разных целей не может быть действительным.

## Закон ФРГ о регулировании защиты и конфиденциальности данных в телекоммуникациях и телемедиях

Ein Service des Bundesministeriums der Justiz und für Verbraucherschutz  
sowie des Bundesamts für Justiz – www.gesetze-im-internet.de

**Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien\* (Telekommunikation-Telemedien-Datenschutz-Gesetz - TTDSG)**

TTDSG

Ausfertigungsdatum: 23.06.2021

Vollzitat:

\*Telekommunikation-Telemedien-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982), das zuletzt durch Artikel 4 des Gesetzes vom 12. August 2021 (BGBl. I S. 3544) geändert worden ist\*

**Hinweis:** Änderung durch Art. 25 G v. 25.6.2021 I 2099 (Nr. 37) textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet  
Änderung durch Art. 4 G v. 12.8.2021 I 3544 (Nr. 54) textlich nachgewiesen, dokumentarisch noch nicht abschließend bearbeitet

\* Dieses Gesetz dient der Umsetzung der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37), die durch Artikel 2 der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. L 337 vom 18.12.2009, S. 11) geändert worden ist.

**Fußnote**

+++ Textnachweis ab: 1.12.2021 +++  
+++ Amtlicher Hinweis des Normgebers auf EG-Recht:  
Besetzung der  
EGRL 58/2002 (CELEX Nr.: 32002L0058) +++

Das G wurde als Artikel 1 des G v. 23.6.2021 I 1982 vom Bundestag mit Zustimmung des Bundesrates beschlossen. Es ist gem. Art. 14 Abs. 1 dieses G am 1.12.2021 in Kraft getreten.

**Inhaltsübersicht**

Teil 1

Allgemeine Vorschriften

§ 1 Anwendungsbereich des Gesetzes  
§ 2 Begriffsbestimmungen

Teil 2

Datenschutz und Schutz der  
Privatsphäre in der Telekommunikation

Kapitel 1

Vertraulichkeit der Kommunikation

- Seite 1 von 24 -

Новый Закон о защите телекоммуникационных данных (TTDSG), вступивший в силу 01.12.2021г., объединяет положения о защите данных в законодательстве о телемедиа и телекоммуникациях, которые ранее были разбросаны по целому ряду законов Германии. Среди прочего, TTDSG регулирует защиту данных при использовании готовой к Интернету терминальной инфраструктуры, такой как веб-сайты, службы обмена сообщениями или устройства «умный дом». С этой целью положения о защите данных Закона о средствах массовой информации (TMG) и Закона о телекоммуникациях (TKG) объединяются в новом TTDSG. Кроме того, TTDSG регулирует обязанности Федерального сетевого агентства и Федерального уполномоченного по защите данных и свободе информации (BfDI). Однако для операторов веб-сайтов и приложений TTDSG не налагает никаких новых обязательств. Скорее, TTDSG предоставляет им разъяснения и большую правовую определенность при обработке (персональных) данных, например, в связи с файлами cookie.

Немецкая конференция по защите данных (DSK) недавно [опубликовала](#) новый [руководящий документ](#) для поставщиков телекоммуникационных услуг по применению TTDSG.

<https://www.gesetze-im-internet.de/ttdsg/>

<https://www.natlawreview.com/article/new-telecommunications-telemedia-data-protection-act-ttdsg>

## Руководство CNIL по лучшим практикам для разработчиков веб-сайтов и мобильных приложений



*To protect personal data, support innovation, preserve individual liberties*

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL  

### The CNIL publishes a GDPR guide for developers

11 June 2020

*In order to assist web and application developers in making their work GDPR-compliant, the CNIL has drawn up a new guide to best practices under an open source license, which is intended to be enriched by professionals.*

>> GDPR GUIDE  
>> FOR DEVELOPERS



**Is this guide only for developers?**

This guide is mainly aimed at developers working alone or in teams, team leaders, service providers but also at anyone interested in web or application development.

It provides advice and best practices, and thus gives useful keys to understand the GDPR for every stakeholder, regardless of the size of their structure. It can also stimulate discussions and practices within the organisations and in customer relationships.

Французский орган по защите данных (CNIL) опубликовал 11 июня 2020 года руководство, которое включает в себя следующие разделы:

1. Develop in compliance with the GDPR
2. Identify personal data
3. Prepare your development
4. Secure your development environment
5. Manage your source code
6. Make an informed choice of architecture
7. Secure your websites, applications and servers
8. Minimize the data collection
9. Manage user profiles
10. Control your libraries and SDKs
11. Ensure quality of the code and its documentation
12. Test your applications
13. Inform users
14. Prepare for the exercise of people's rights
15. Define a data retention period
16. Take into account the legal basis in the technical implementation
17. Use analytics on your websites and applications



## Рекомендации CNIL по использованию чат-ботов на вебсайтах и в мобильных приложениях



Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL | 🔍 | 🌐 | 📱

🏠 > Chatbots : les conseils de la CNIL pour respecter les droits des personnes

### Chatbots : les conseils de la CNIL pour respecter les droits des personnes

19 février 2021

*De plus en plus présents sur les sites web et applications, les chatbots permettent de fournir rapidement des réponses aux utilisateurs. Leur mise à disposition, qui peut présenter des enjeux importants pour les droits des personnes, doit respecter certaines règles.*

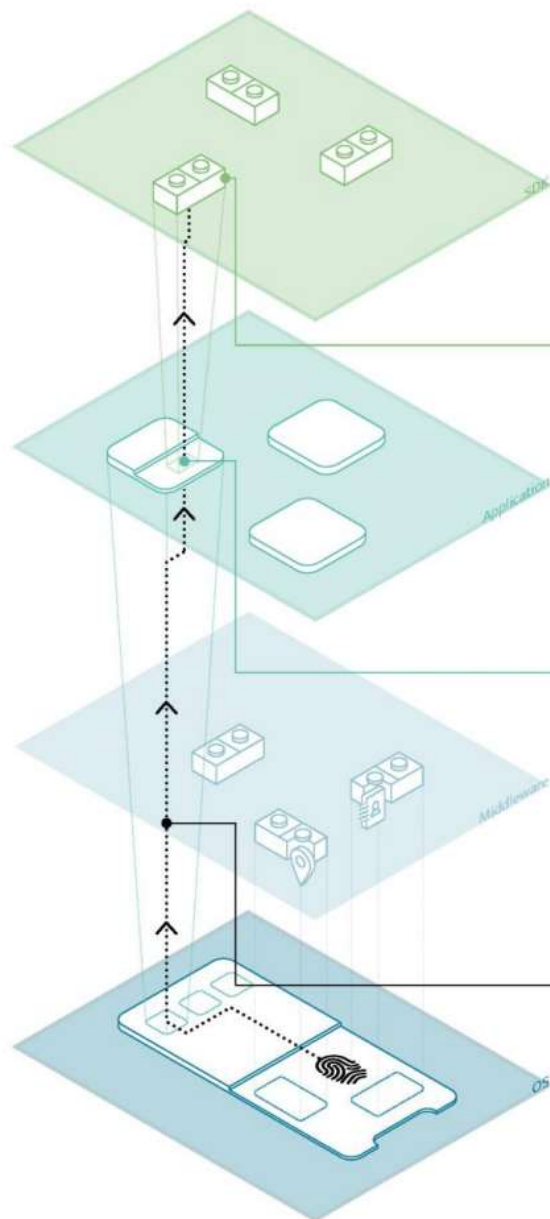


Les agents conversationnels (ou *chatbots*) sont des logiciels permettant le dialogue d'un utilisateur avec un programme destiné à lui fournir des informations. Ils servent à apporter des réponses aux questions les plus fréquentes, tout en dispensant cette information d'une manière ciblée, pertinente et interactive. Pour cela, des données personnelles sont souvent traitées, par exemple pour conserver une trace de la conversation, même si le service est disponible sans créer de compte ou sans fournir d'informations directement identifiantes.

Французский надзорный орган Commission nationale de l'informatique et des libertés (CNIL) 19.02.2021 опубликовал рекомендации по использованию чат-ботов, ключевые положения которых:

- использование файлов cookie для функций чат-бота должно соответствовать общим принципам, изложенным в соответствующем руководстве CNIL;
- данные из чат-бота должны храниться в течение времени, необходимого для достижения цели обработки, определенной контролером;
- использование субъекта чат-бота не должно приводить к автоматическому принятию значимых решений в отношении субъекта (затрагивающих его правовое положение или интересы, например, отказ в онлайн-заявке на кредит, применение более высоких кредитных ставок или невозможность подать заявку на замещение вакансии) без учета требований ст.22 GDPR;
- некоторые чат-боты предоставляют субъекту возможность ввода информации в свободной форме, которая может содержать чувствительные категории данных. В этом случае необходимо применять компенсирующие механизмы, например, предварительный показ уведомления с призывом к субъектам воздерживаться от ввода чувствительных данных, осуществления немедленной или регулярного уничтожения истории переписки в чат-боте (если это приемлемо с т.з. цели и контекста обработки данных).

## Recommandations CNIL по соблюдению GDPR в мобильных приложениях



### Lecture et traitement d'un identifiant mobile par un SDK pour le compte de l'éditeur et pour son propre compte.

Un éditeur d'application fait appel aux services d'un fournisseur de SDK pour faciliter le développement de son application. Celui-ci introduit un SDK dans l'application ayant pour fonctionnalité d'accéder à l'identifiant publicitaire unique du mobile afin de pouvoir suivre le comportement de l'utilisateur dans l'application.

#### Finalité SDK

Amélioration du service de profilage des utilisateurs

#### Responsabilités

▶ Le fournisseur de SDK est responsable de traitement

Il ne peut effectuer ces traitements que si l'éditeur, responsable de traitement initial, lui en a donné l'autorisation.

#### Finalité éditeur

Monétisation des espaces publicitaires

#### Responsabilités

▶ L'éditeur d'application est responsable de traitement

▶ Le fournisseur de SDK est sous-traitant

#### Finalités déterminées conjointement

Accès à l'identifiant publicitaire

#### Responsabilités

▶ L'éditeur d'application est co-responsable de traitement

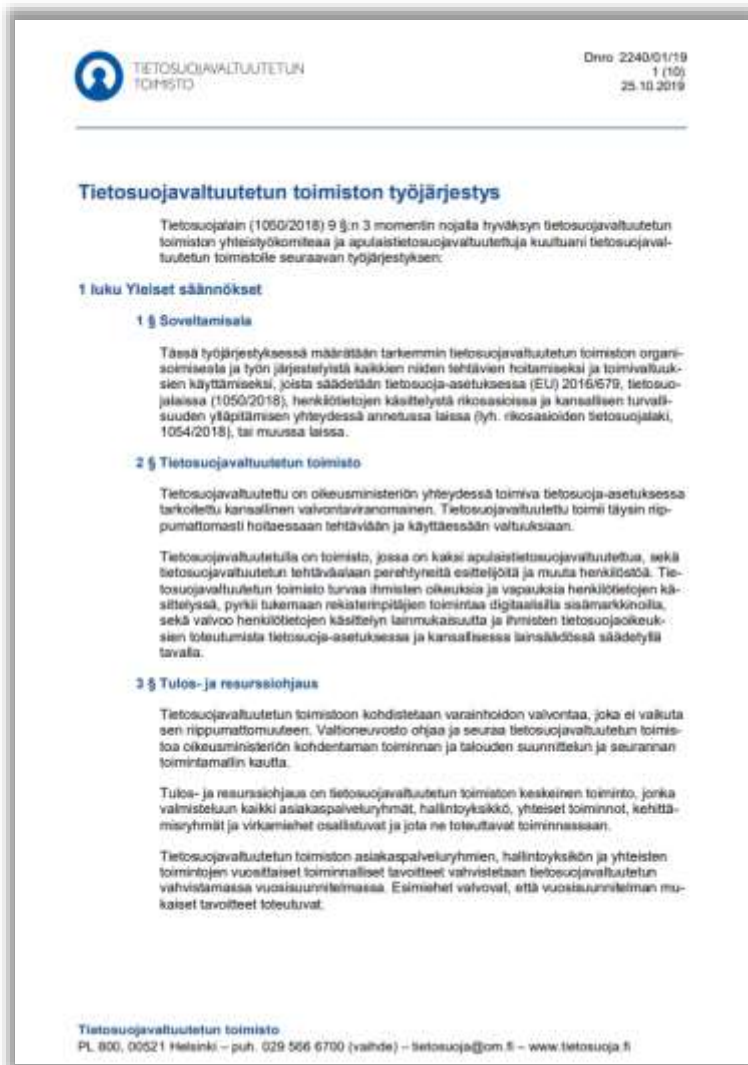
▶ Le fournisseur de SDK est co-responsable de traitement

## 323 ПО от EDPS для проверки соблюдения веб-сайтами требований GDPR

The screenshot shows the 'Website Evidence Collector' page on the 'joinup' platform. The page header includes the European Commission logo and navigation links for 'Interoperable Europe', 'Interoperability Solutions', 'Sign In', and 'Get started'. The main title is 'Website Evidence Collector' with a 'Subscribe to this solution' button and a 'Download releases' link. Below the title, there are tags for 'Free and open source software', 'Topics: Reusable Software Components, Open Source Software, ICT security', and 'Downloads: 3534'. The page has tabs for 'Overview', 'Members', and 'About'. A 'Like (2)' button is visible. A text block describes the tool: 'The European Data Protection Supervisor (EDPS) publishes the tool Website Evidence Collector under the European Union Public License (EUPL-1.2). The tool supports the automation of privacy and personal data protection inspections of websites. The EDPS welcomes any feedback and suggestions for improvements to be sent to: tech-privacy@edps.europa.eu. The tool collects evidence of personal data processing, such as cookies, or requests to third parties. The collection parameters are configured ahead...'. Below this is a 'Read more' link. A 'Releases' section is shown with a 'Show archived' toggle. The releases are listed in a grid of 8 items, each with a version number, release date, and status.

Version	Release Date	Status
v2.1.1	20/09/2023	Completed
v2.1.0	06/09/2023	Completed
v2.0.0	30/06/2023	Completed
v1.9.0	11/01/2021	Completed
v0.4.0	20/01/2020	Under development
v0.3.1	18/10/2019	Under development
v0.3.0	30/05/2019	Under development
v0.3.1	31/07/2019	Work development

## Финский омбудсмен выразил опасения в отношении инструментов для анализа данных пациентов



Управление омбудсмана по защите данных ("Омбудсмен") в Финляндии 27.10.2022 опубликовало результаты оценки двух случаев, когда медицинские учреждения планировали использовать инструменты для анализа данных пациентов с помощью компьютера с целью выявления потребностей в медицинском обслуживании. Системы должны выявлять тех пациентов, у которых есть риск для здоровья, и в этом случае медицинский работник сможет оценить необходимость направления их на лечение, в то время как пациенты, у которых риск для здоровья не будет выявлен на основе алгоритмов, не будут отбираться для более детальной оценки. Анализ данных о пациентах также будет использоваться, например, для прогнозирования потребности в медицинских услугах и заболеваемости на популяционном уровне.

В этом контексте омбудсмен предупредил поставщиков медицинских услуг, что операционный метод, предназначенный для выявления риска для здоровья отдельного пациента, вероятно, не будет соответствовать требованиям правил защиты данных в его нынешнем виде. Кроме того, омбудсмен считал, что в связи с выявлением рисков для здоровья пациентов будут возникать автоматизированные решения, которые операторы не признали. Наконец, омбудсмен заявил, что преимущества инструментов, способствующих укреплению общественного здоровья и здоровья пациентов, очевидны, но в то же время их использование должно быть согласовано с нормативными актами, касающимися обработки персональных данных и правовой защиты пациентов и их права на самоопределение.

## 325 Решение Datatilsynet по делу DMI

Датский надзорный орган в сфере персональных данных (Datatilsynet) 11.02.2020 опубликовал информацию о своем решении в отношении жалобы пользователя сайта Датского Метеорологического Института (DMI) на непропорциональную обработку его персональных данных в рекламных целях. Позиция датского надзорного органа во многом совпадает с другими европейскими DPA, но есть и особенности:

1. Опираясь на решения CJEU по делам *Wirtschaftsakademie* и *Fashion ID*, Datatilsynet пришел к выводу, что контролера веб-сайта (DMI) вместе с Google следует рассматривать как совместных контролеров, но только в отношении сбора и раскрытия данных посетителей веб-сайта DMI, а вот любая последующая обработка данных, включая профилирование, Google уже осуществляет без влияния DMI - как самостоятельный контролер.

2. Datatilsynet подверг критике cookie-баннер DMI, в котором пользователю предлагается только две опции: нажать «ОК», тем самым дав согласие на сбор файлов cookie как для статистических, так и для маркетинговых целей, или «Показать подробности», дав отдельное согласие на каждую из категорий файлов cookie. Такие опции не отвечают требованиям прозрачности и гранулярности согласия (пользователя косвенно подталкивают к даче согласия на использование всех файлов cookie), так как пользователь фактически лишен возможности дать отдельное согласие при первоначальном взаимодействии с cookie-баннером. Иначе говоря, возможность воздержаться от предоставления согласия на обработку персональных данных в cookie-баннере DMI не имеет такого же коммуникационного эффекта, как возможность дать согласие.

3. Было указано, что субъекты данных должны быть в простой и легко понятной форме осведомлены о контролерах и целях обработки файлов cookie. Так, в описании маркетинговых файлов cookie кратко описывается их поставщик (DoubleClick) и нет достаточно четкой информации о том, что для таких файлов совместными контролерами являются Google и DMI. Вместо этого пользователям предоставлялись часто непонятные или избыточные для них сведения о веб-сайтах, псевдонимах или названиях продуктов, используемых контролером.



### FAQ zu Facebook-Fanpages

Stand: 22. Juni 2022

#### 1. Was genau ist eine Facebook-Seite bzw. eine Fanpage?

Unternehmen, Marken, Gruppierungen oder Personen des öffentlichen Lebens verwenden Facebook-Fanpages – auch Facebook-Seiten genannt – für die eigene Präsentation auf der Plattform Facebook.

Davon abzugrenzen sind die reinen Facebook-Profilen der registrierten Nutzenden, die Privatpersonen zugeordnet sind.

Während ein Profil weitestgehend zu privaten Zwecken eingerichtet wird, werden Facebook-Fanpages im geschäftlichen / nicht-privaten Kontext betrieben. Facebook-Fanpages ersetzen, gerade bei Kleinunternehmungen, in nicht wenigen Fällen die klassische Unternehmenswebseite oder ergänzen diese.

#### 2. Warum ist der Betrieb von Facebook-Fanpages datenschutzrechtlich problematisch?

Meta Platforms als Betreiber des Dienstes Facebook verarbeitet die Daten der Nutzenden nicht ausschließlich zum Zweck der Bereitstellung eines sozialen interaktiven Netzwerks, sondern auch zu Werbezwecken, die auf feingranularen Profilen der Nutzenden aufsetzen, um für sie „passgenaue“ Werbung im Auftrag von Unternehmen, Verbänden, Parteien etc. schalten zu können. Welche personenbezogenen Daten in welcher Art und Weise konkret verarbeitet werden, bleibt allerdings weitestgehend unklar.

Конференция немецких надзорных органов по защите данных ("Datenschutzkonferenz") 22.06.2022 опубликовала свои разъяснения в связи с использованием фан-страниц (fanpage) Facebook, согласно которым эти страницы должны быть деактивированы, если их соответствие GDPR не может быть обеспечено.

◇ Meta Platforms Inc., как оператор Facebook, обрабатывает данные пользователей, среди прочего, для рекламных целей, которые основаны на профилях пользователей, чтобы иметь возможность размещать индивидуально подобранную рекламу от имени компаний, ассоциаций и других лиц. Однако остается неясным, какие персональные данные и каким образом обрабатываются.

◇ Ранее Суд Европейского Союза в деле Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH (C-210/16) установил, что администраторы фан-страниц Facebook выступают в качестве совместных контролеров с Meta Platforms, и поэтому они должны заключить соглашение о совместном контроле.

◇ Текущее соглашение, представленное Meta Platforms, не соответствует требованиям ст.26 GDPR. Поэтому администраторы фан-страниц Facebook в настоящее время не могут обеспечить и доказать, что обработка данных, за которую они несут ответственность, происходит на законных основаниях.

◇ Таким образом, администраторам фан-страниц Facebook остается единственный выход - деактивировать свои фан-страницы до тех пор, пока они не смогут выполнить свои обязательства согласно нормам GDPR.

## Рекомендации Комитета министров СЕ по автоматической обработке данных в контексте профилирования



MINISTERS' DEPUTIES      Recommendations      CM/Rec(2021)8      3 November 2021

### **Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling**

*(Adopted by the Committee of Ministers on 3 November 2021  
at the 1416<sup>th</sup> meeting of the Ministers' Deputies)*

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that digital technologies allow the large-scale processing of data, including personal data, in both the public and private sectors, used for a wide range of purposes including for services widely accepted and valued by society and individuals;

Noting that data are processed in particular by calculation, comparison, correlation and other statistical techniques, with the aim of producing profiles or models that could be used in many ways for different purposes and uses, by matching the data of several individuals;

Considering that, by observing and linking a large amount of data, even anonymous data, profiling techniques can have an impact on the data subjects by placing them in predetermined categories, very often without their knowledge;

Considering that the lack of transparency – or even invisibility – of profiling, and the lack of accuracy that may derive from the automatic application of pre-established rules of inference, can pose significant risks for individuals' rights and freedoms;

Noting that the data processed in the context of profiling may include special categories of personal data, notably biometric data, the misuse of which can cause irreversible damage to data subjects, since such data can be used to access various services and can have legal consequences;

Considering in particular that the protection of fundamental rights, notably the rights to privacy and to protection of personal data, safeguards the existence of different and independent spheres of life where each individual can control his or her information;

Considering the particular vulnerability of some of the persons profiled, including children, and the possible seriousness of the consequences of such profiling, sometimes for the rest of their lives;

Aware of the intensification and diversification of the profiling of individuals, in all spheres of activity;

03.11.2021 года Комитет министров Совета Европы (Council of Europe) утвердил Рекомендации CM/Rec(2021)8 о соблюдении принципов соблюдения информационной приватности субъектов персональных данных при их профилировании.

## Запрет Facebook и Instagram показывать пользователям персонализированную рекламу без их согласия

### EU set to bar Meta from ads based on personal data

By Foo Yun Chee and Chavi Mehta



Woman holds smartphone with Meta logo in front of a displayed Facebook's new rebrand logo Meta in this illustration picture taken October 28, 2021. REUTERS/Dado Ruvic/Illustration/File Photo

BRUSSELS/BANGALORE, Dec 6 (Reuters) - Meta (**META.O**) will only be able to run advertising based on personal data with users' consent, according to a confidential EU privacy watchdog decision, a person familiar with the matter said on Tuesday, in a blow to the U.S. social network.

The Irish data protection agency, which oversees Meta because its European headquarters is located in Dublin, has been given a month to issue a ruling based on the European Data Protection Board's (EDPB) binding decision.

Европейские надзорные органы считают, что соцсети Facebook и Instagram (принадлежат Meta) смогут показывать рекламу, основанную на персональных рекомендациях, только с согласия пользователей.

Модель таргетированной рекламы в соцсетях, основанной на анализе большого количества данных, привлекла пристальное внимание регулирующих органов по всему миру. Ирландский надзорный орган ('DPC') рассматривал этот вопрос ещё с 2018 года и в результате решил, что Meta игнорирует требования властей об использовании персональных данных.

DPC также постановил, что Meta должна разрешить пользователям отказаться от предоставления своих персональных данных для таргетирования рекламы. Компании по-прежнему будет разрешено использовать неперсонализованные данные, а также запрашивать согласие пользователей на обработку персональных данных.



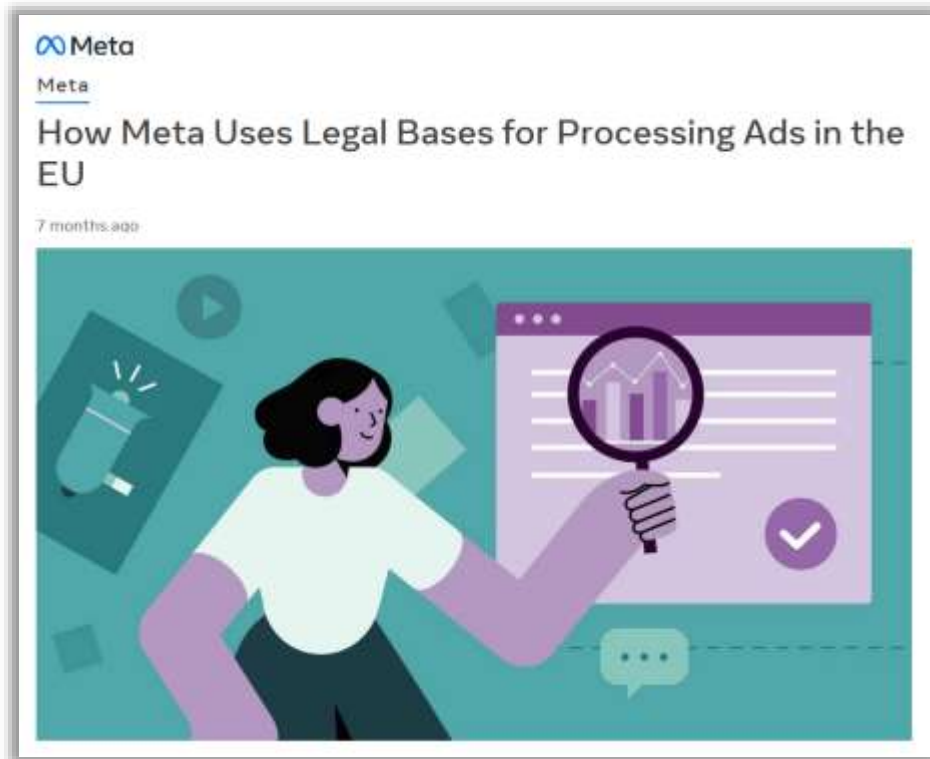
## Норвежский Datatilsynet временно запретил Facebook отслеживать данные пользователей для настройки рекламы

Норвежское управление по защите данных (Datatilsynet) выявило, что Facebook и Instagram "собирают личную информацию крайне деликатного свойства посредством непрозрачных и навязчивых способов мониторинга". Согласно распоряжению ведомства от 14.07.2023, вступающему в силу в августе сроком на три месяца, пользователи в королевстве не будут видеть в социальных сетях персонализированную рекламу, основанную на их онлайн-активности и геолокации.

Facebook и Instagram вправе показывать рекламу, но ее подбор будет основываться на информации, которую сами пользователи указали в разделе "О себе". За нарушение предписания Meta грозит штраф в €88,7 тыс. в сутки.



### 330 Meta перестанет показывать индивидуализированную рекламу без согласия



Об этом компания объявила на своём сайте: основание обработки персональных данных для такой рекламы будет изменено с законного интереса на согласие. Конкретная дата для такого перехода пока не называется.

Ранее, с 5 апреля этого года компания обрабатывала такие данные на основании законного интереса, а до этого изначально — на основании договора (пользовательского соглашения).

Однако изначальная практика была признана надзорным органом незаконной по жалобе активистов из NOYB.

Теперь же, после дополнительных консультаций с надзорным органом Мета решила перейти к подходу, на котором изначально настаивали прайваси-активисты.

Решение касается пользователей из ЕС, Европейской экономической зоны и Швейцарии.


## 331 EDPB запретил Meta обработку данных для поведенческой рекламы

**EDPB Urgent Binding Decision on processing of personal data for behavi**

3 November 2023 EDPB

On 27 October, the EDPB adopted an urgent binding decision instructing the Irish (IE) DPA as lead supervisory authority (LSA) to take, within two weeks, final measures regarding Meta Ireland Limited (Meta IE) and to impose a ban on the processing of personal data for behavioural advertising on the legal bases of contract and legitimate interest across the entire European Economic Area (EEA).

The urgent binding decision followed a request from the Norwegian Data Protection Authority (NO DPA) to take final measures in this matter that would have effect in the entire European Economic Area (EEA).



The ban on processing will become effective one week after the notification of the final measures by the IE SA to the controller.

The Irish DPC has notified Meta on 31/10 about the EDPB Urgent Binding Decision.

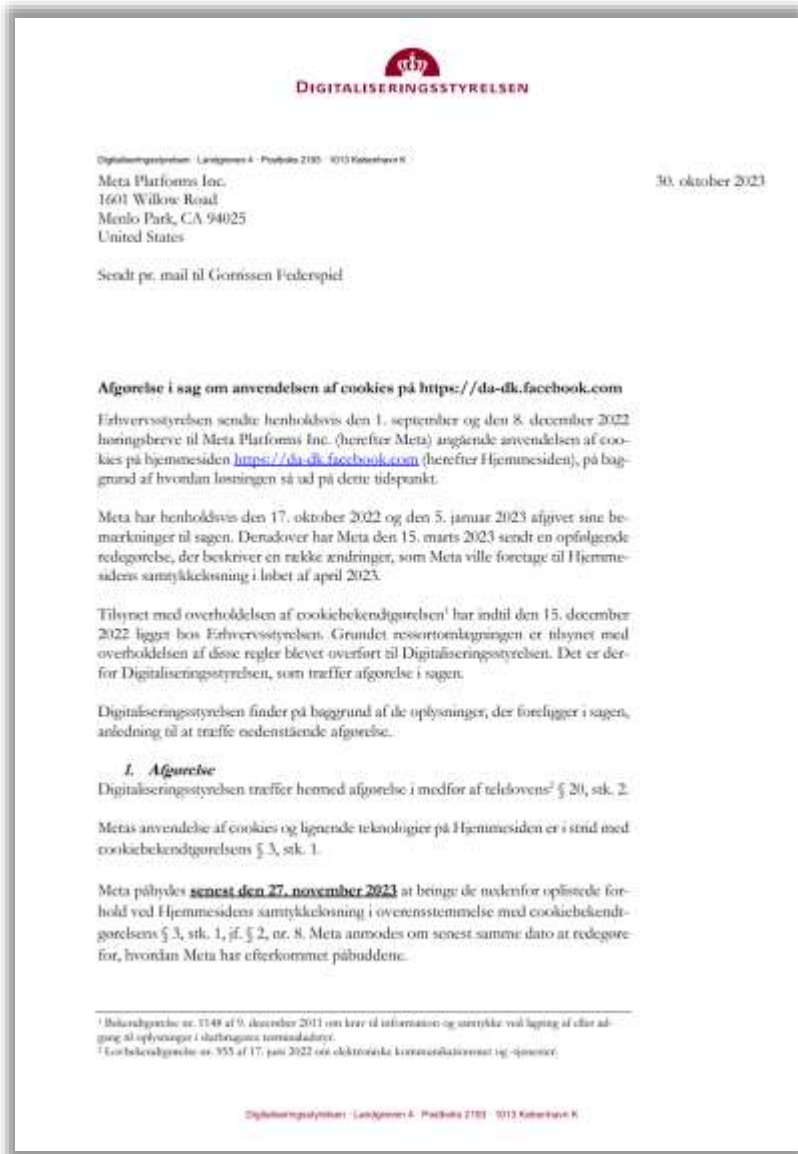
The EDPB takes note of Meta's proposal to rely on a consent based approach as legal basis, as it was reported on 30/10. The Irish DPC is currently evaluating this together with the Concerned Supervisory Authorities (CSAs).

EDPB Chair Anu Talus said: "After careful consideration, the EDPB considered it necessary to instruct the IE SA to impose an EEA-wide processing ban, addressed to Meta IE. Already in December 2022, the EDPB Binding Decisions clarified that contract is not a suitable legal basis for the processing of personal data carried out by Meta for behavioural advertising. In addition, Meta has been found by the IE SA to not have demonstrated compliance with the orders imposed at the end of last year. It is high time for Meta to bring its processing into compliance and to stop unlawful processing."

◇ Европейский совет по защите данных (European Data Protection Board, EDPB) предписал европейскому надзорному органу, ирландской комиссии по защите данных (Data Protection Commission, DPC), ввести запрет для Meta на обработку персональных данных, используемых в «поведенческой рекламе», на всей территории Европейской экономической зоны (страны ЕС, а также Исландия, Норвегия и Лихтенштейн).

◇ Еще в декабре 2022 года со стороны EDPB было разъяснено, что договор не является подходящим правовым основанием для обработки персональных данных, осуществляемой компанией Meta в целях поведенческой рекламы.

## 332 Предписание Meta и Google исправить нарушения требований к cookies в Дании



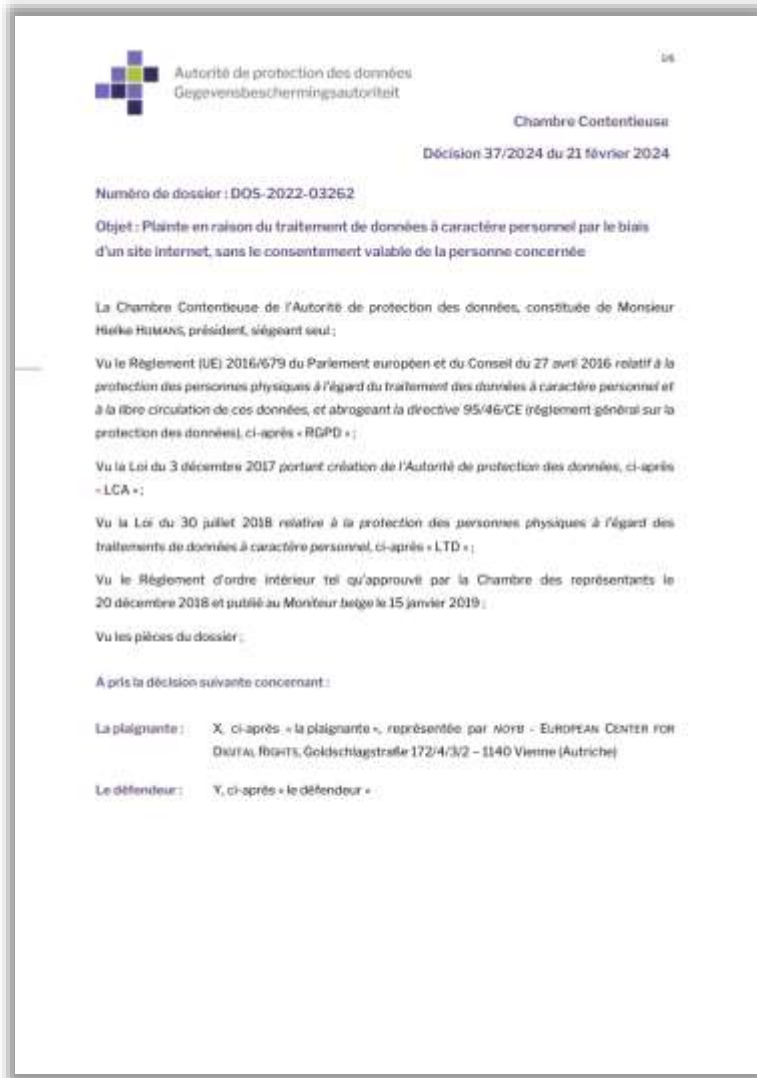
Датское цифровое агентство (Digitaliseringsstyrelsen) 30.10.2023 вынесло предписание в отношении компаний Meta Platforms Inc. и Google LLC за нарушение Постановления о cookie-файлах (Cookie Order), поскольку выявлено:

- ◇ получение общего согласия на использование файлов cookie для нескольких различных целей, не позволяя конечным пользователям давать конкретное согласие для каждой отдельной цели;
- ◇ отсутствие возможности отзыва согласия в понятной и удобной для пользователя форме;
- ◇ отсутствие исчерпывающей информации об используемых файлах cookie и аналогичных технологиях.

Digitaliseringsstyrelsen предписал в течение 4 недель выполнить следующие действия для устранения нарушений:

- ◇ изменить порядок получения согласий, чтобы пользователи могли давать отдельное согласие для разных целей;
- ◇ предоставить конечным пользователям возможность отозвать свое согласие на использование файлов cookie и аналогичных технологий и сделать эту возможность понятной и постоянно доступной на сайте;
- ◇ предоставлять пользователям постоянный доступ к информации обо всех используемых файлах cookie и аналогичных технологиях на ясном, четком и понятном языке.

## Бельгийский APD заключил мировые соглашения с медиа-сайтами о коррективке cookie-баннеров



Управление по защите данных Бельгии (APD) 21.02.2024 не удовлетворило жалобу на отсутствие кнопки "Отклонить все" на первом уровне cookie-баннера, поскольку кнопка "Подтвердите мой выбор" означала, что cookie не размещаются, так как ни одна из категорий несущественных данных не была отмечена по умолчанию. Нажатие на кнопку "Подтвердить мой выбор" означало, что файлы cookie не будут размещены, точно так же, как и кнопка, позволяющая отклонить несущественные файлы cookie.

APD также отметило, что cookie-баннер можно было вызвать в любой момент во время посещения сайта с помощью плавающего значка в левом нижнем углу веб-страницы, чтобы изменить настройки cookie. Кроме того, с момента подачи жалобы контроллер также добавил кнопку "Отклонить все".

## Бельгийский APD о cookie-баннере: кнопка "Подтвердить мой выбор" эквивалентна кнопке "Отклонить все"



Управление по защите данных Бельгии (APD) 01.12.2023 опубликовало четыре соглашения с медиа-сайтами об использовании файлов cookie, которые были заключены по жалобам, поданным организацией None Of Your Business (NOYB). В начале этого года NOYB подала жалобы на ряд бельгийских медиакомпаний в связи с тем, как на их веб-сайтах используются файлы cookie и баннеры cookie.

Проанализировав ответы на предложения об урегулировании, бельгийский APD принял решение об условиях урегулирования. APD отклонил просьбы NOYB об изменении условий урегулирования, в том числе просьбу о наложении штрафов на компании. Вместо этого с компаниями были заключены мировые соглашения по внесению изменений в баннеры cookie на их сайтах, а именно:

- ◊ разместить кнопку "Отказаться от всего" рядом с кнопкой "Принять все";
- ◊ не делать кнопку "принять все" визуально более жирной, чем другие варианты;
- ◊ гарантировать, что процедура отзыва согласия не требует большего количества кликов, чем процедура предоставления согласия.

<https://www.autoriteprotectiondonnees.be/publications/transaction-art95-n-161-2023.pdf>

<https://www.autoriteprotectiondonnees.be/publications/transaction-art95-n-162-2023.pdf>

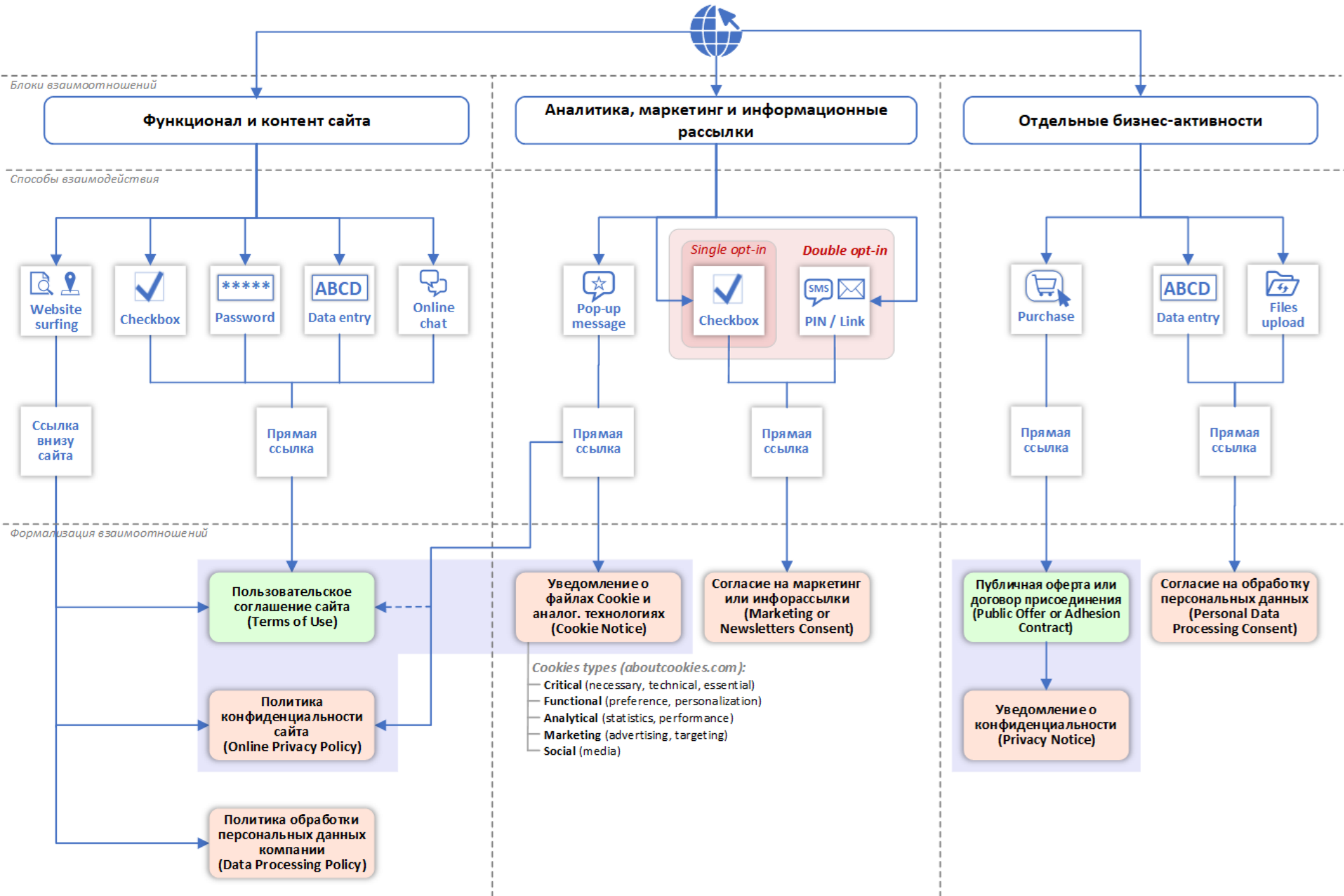
<https://www.autoriteprotectiondonnees.be/publications/transaction-art95-n-160-2023.pdf>

<https://www.autoriteprotectiondonnees.be/publications/transaction-art95-n-159-2023.pdf>

### 335 Подборка статей и материалов о профилировании

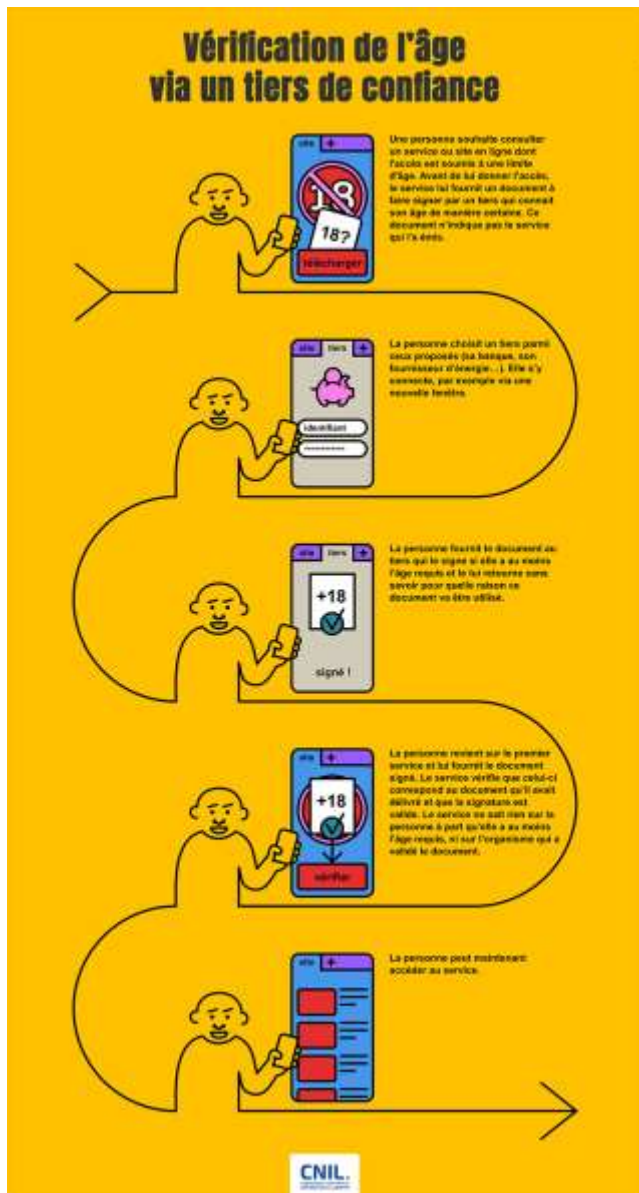
- [Profiling with big data: Identifying privacy implications for individuals, groups and society](#)
- [A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case](#)
- [Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination](#)
- [Challenges and Legal Gaps of Genetic Profiling in the Era of Big Data](#)
- [Profiling as inferred data. Amplifier effects and positive feedback loops](#)
- [A Study of Event Frequency Profiling with Differential Privacy](#)
- [Privacy aware and faceted user-profile management using social data](#)
- [How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies](#)
- [Social network data analysis to highlight privacy threats in sharing data](#)
- [GDPR for marketers: Profiling](#)
- [ICO \(UK\) on automated decision-making and profiling](#)
- [CMA \(UK\) on how algorithms can reduce competition in digital markets and harm consumers](#)
- [CDEI \(UK\) review into bias in algorithmic decision-making](#)
- [Decision of the Court of Amsterdam \(Case C/13/696010/ HA ZA 21-81, 14 April 2021\) concerning order to Uber Technologies Inc. to reinstate drivers dismissed by an algorithm in the UK](#)

# 336 Взаимодействие с субъектами посредством сайтов





## Рекомендации от CNIL по разработке технических решений для проверки возраста пользователей



Рекомендации французского надзорного органа (CNIL) по разработке технических решений для проверки возраста пользователей были опубликованы 26.07.2022. Следование рекомендациям должно обеспечить тройную защиту приватности пользователя интернет-ресурса:

- ◇ провайдер сервиса по идентификации может установить личность пользователя, но не знает, к какому ресурсу он обращается;
- ◇ провайдер сервиса по подтверждению возраста пользователя для владельца ресурса, может знать ресурс или услугу, к которой обращается пользователь, но не может идентифицировать пользователя;
- ◇ владелец ресурса, которому необходимо проверить возраст, знает, что пользователь является совершеннолетним и что он обращается к ресурсу, но не может идентифицировать пользователя.

## 338 Файлы cookies в европейском правовом поле защиты данных



**Table 1: cookies used by commonly used website**

Web Site / Technique	Cookies-Checker	Firefox	Chrome
Facebook	Unable	12 FPC; 0 TCP	9 FPC; 2 TCP
Google	2 FPC; 0 TPC	8 FPC; 0 TCP	4 FPC; 1 TCP
Amazon.com	7 FPC; 0 TPC	11 FPC; 0 TCP	7 FPC; 4 TCP
Linkedin	8 FPC; 0 TPC	14 FPC; 0 TCP	9 FPC; 3 TCP
Twitter	4 FPC; 0 TPC	9 FPC; 0 TCP	6 FPC; 3 TCP
YouTube	4 FPC; 0 TPC	12 FPC; 0 TCP	6 FPC; 6 TCP
Instagram	11 FPC; 0 TPC	10 FPC; 12 TCP	2 FPC; 2 TCP
The Guardian	8 FPC; 6 TPC	2 FPC; 0 TCP	2 FPC; 11 TCP
WSJ	27 FPC; 8 TPC	6 FPC; 0 TCP	7 FPC; 5 TCP
En.wikipedia	3 FPC; 0 TPC	3 FPC; 0 TCP	3 FPC; 2 TCP
Leibniz University	2 FPC; 0 TPC	1 FPC; 0 TCP	1 FPC; 1 TCP
University of Oslo	6 FPC; 0 TPC	1 FPC; 0 TCP	6 FPC; 0 TCP
PornHub	1 FPC; 1 TPC	9 FPC; 4 TCP	9 FPC; 9 TCP

Note: FPC: First Party Cookies, TPC: Third Party Cookies

<https://www.duo.uio.no/bitstream/handle/10852/67266/Thesis-Completed.pdf?sequence=1&isAllowed=y>

Информация о пользовательских данных, которые можно собирать с использованием Firebase (Google Analytics) - [https://support.google.com/firebase/topic/6317484?hl=ru&ref\\_topic=6386699](https://support.google.com/firebase/topic/6317484?hl=ru&ref_topic=6386699)

Импорт данных в Google Analytics - [https://support.google.com/analytics/topic/6065609?hl=ru&ref\\_topic=1727148](https://support.google.com/analytics/topic/6065609?hl=ru&ref_topic=1727148)



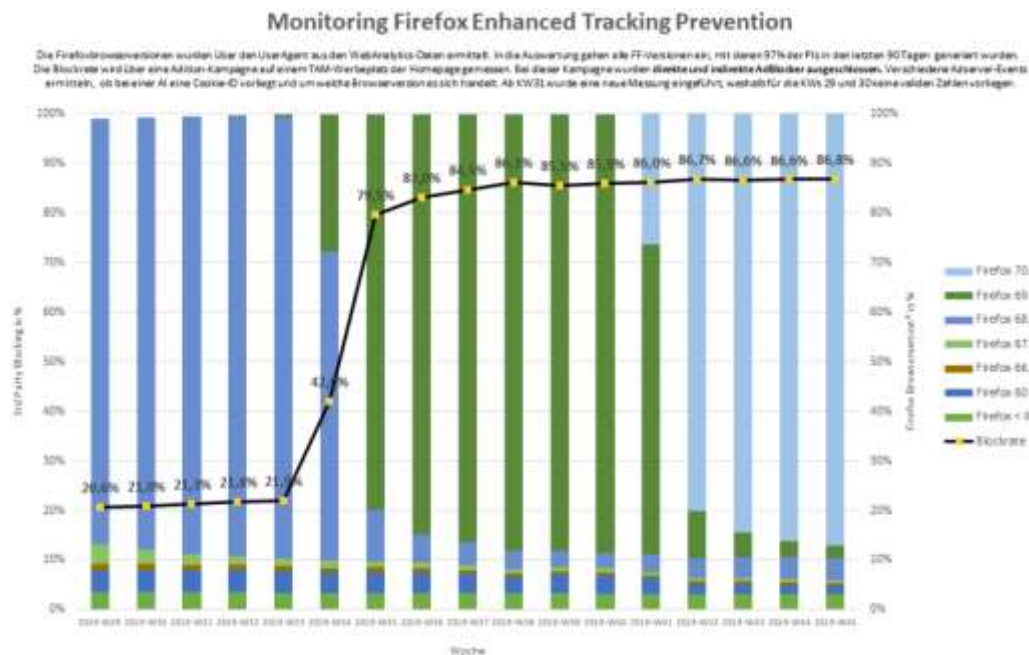
Table 6 Requirements for a valid consent on consent banner design, assessment and source

Requirements		Assessment	Sources at low-level requirement			Location in the paper (page)
High-Level Requirements	Low-Level Requirements	Manual (M), Technical (T) or User study (U)	Binding	Non-binding	Interpretation: Legal (L) or Computer Science (CS)	
Prior	R1 Prior to storing an identifier	M (partially) or T (partially)	✓	✓	-	17
	R2 Prior to sending an identifier	T (partially)	-	-	CS	19
Free	R3 No merging into a contract	M (fully) or T (partially)	✓	✓	-	22
	R4 No tracking walls	M (fully)	-	✓	-	24
Specific	R5 Separate consent per purpose	M (fully)	✓	✓	-	28
Informed	R6 Accessibility of information page	M (fully) or T (partially) together with U	-	✓	-	34
	R7 Necessary information on BTT	M (fully) or T (partially)	✓	✓	-	35
	R8 Information on consent banner configuration	M (fully) or T (partially)	-	✓	-	37
	R9 Information on the data controller	M (fully) or T (partially)	✓	✓	-	38
	R10 Information on rights	M (fully) or T (partially)	✓	✓	-	39
Unambiguous	R11 Affirmative action design	Combination of M and T (partially)	✓	✓	-	40
	R12 Configurable banner	M or T (partially)	-	✓	L	43
	R13 Balanced choice	M (fully)	-	✓	L	45
	R14 Post-consent registration	T (partially)	-	✓	CS	47
	R15 Correct consent registration	Combination of M and T (partially)	-	✓	CS	49
Readable and accessible	R16 Distinguishable	M (fully) or T (partially)	✓	✓	-	52
	R17 Intelligible	U	✓	✓	-	52
	R18 Accessible	U	✓	✓	-	52
	R19 Clear and plain language	U	✓	✓	-	53
	R20 No consent wall	M (fully) or T (partially)	-	✓	L	53
Revocable	R21 Possible to change in the future	M (fully)	✓	✓	-	57
	R22 Delete "consent cookie" and communicate to third parties	Not possible	-	-	CS	59

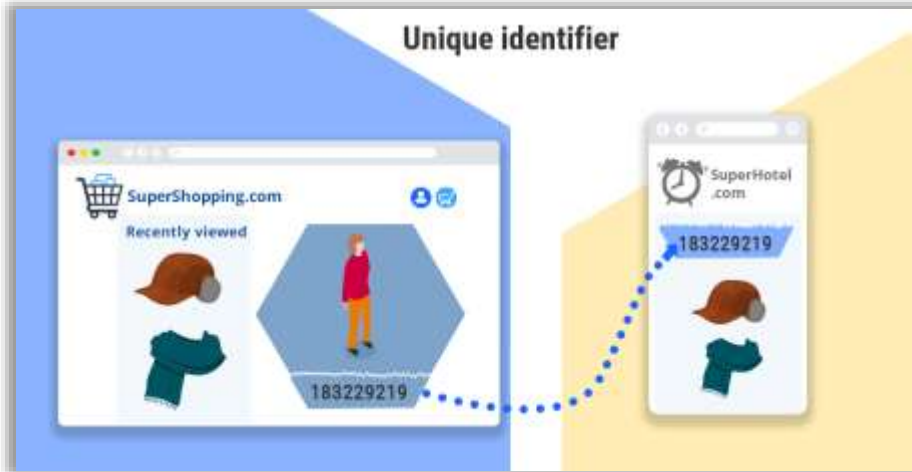
## Руководство IAB по эре, наступающей после отказа от использования сторонних файлов cookie



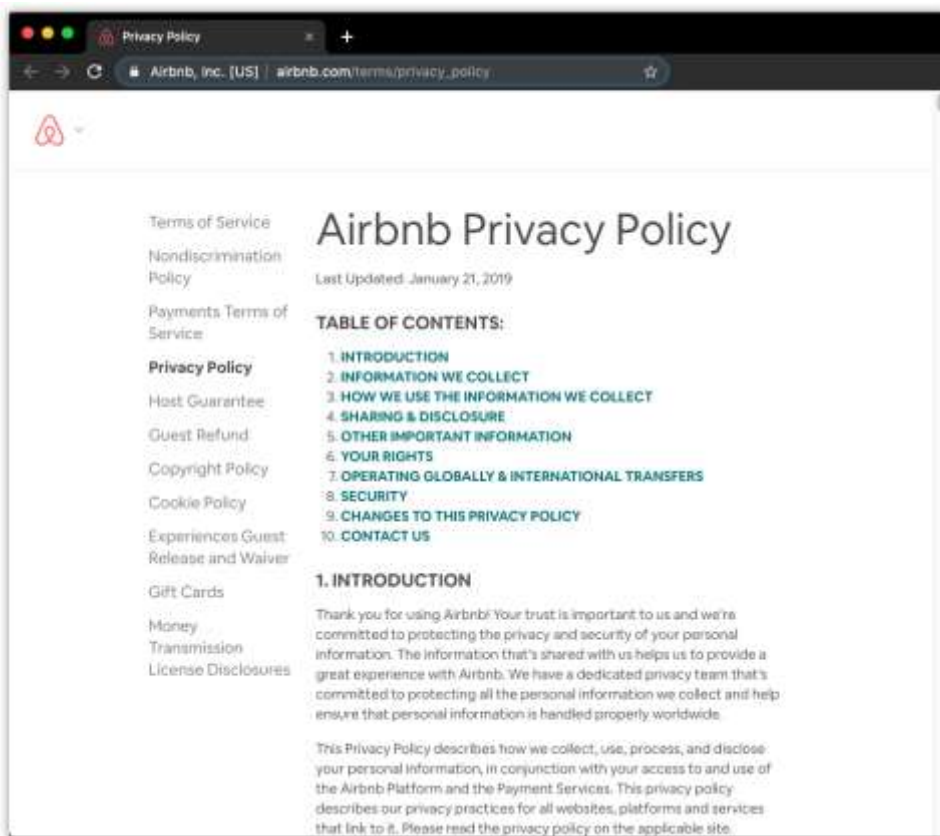
Европейское бюро интерактивной рекламы (Interactive Advertising Bureau - IAB) 10.03.2022г. опубликовало обновленное Руководство по эре, наступающей после отказа от использования сторонних файлов cookie (Guide to the Post Third-Party Cookie Era). В руководстве рассматриваются факторы, способствующие отказу от использования сторонних файлов cookie, влияние закрытых платформ (экосистем) файлов cookie на рекламный бизнес, а также последствия отказа от таких платформ. Кроме того, в руководстве представлен обзор альтернатив для использования сторонних файлов cookie, таких как контекстный таргетинг и рекламные идентификаторы.



# 341 CNIL об альтернативах использования сторонних файлов cookie



## 342 Общие советы по написанию Privacy Policy от Emily Gaston



По мнению автора исследования Политика конфиденциальности должна содержать следующие разделы:


- принципы обработки данных;
- категории обрабатываемых данных;
- цели обработки данных;
- правовые основания сбора данных;
- третьи лица, получающие доступ к данным;
- обеспечение конфиденциальности детей;
- права потребителей в отношении данных;
- контактная информация.

## 343 Сервисы по предупреждению об использовании cookies



The screenshot shows the Cookiebot website. At the top, there is a navigation menu with links for 'What is CCPA?', 'What is GDPR?', 'Pricing', and 'Help'. The main heading is 'Is my website compliant?' in large white text on a blue background. Below the heading, there is a paragraph explaining that the General Data Protection Regulation (GDPR) applies to all websites with users from the EU. A search bar with the placeholder 'Your website address' and a blue button labeled 'CHECK MY WEBSITE' is located at the bottom.

<https://www.cookiebot.com/en/>



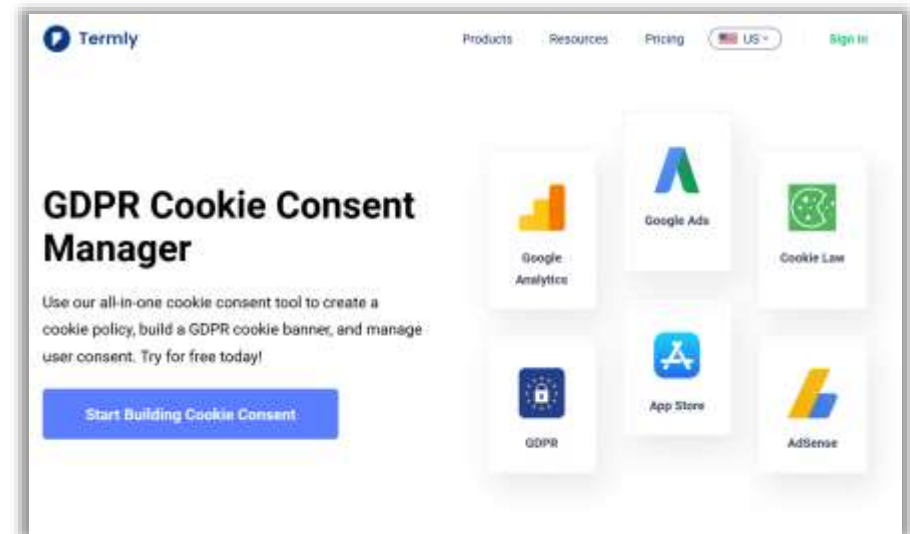
The screenshot shows the CookiePro website. The top navigation includes 'Contact', 'Manage Subscription', 'Login', and 'Pricing'. The main heading is 'Cookie Consent & Website Scanning' in large white text. Below it, there are sub-headings: 'Cookie Banner | Cookie Preferences | Cookie Consent'. A search bar with the placeholder 'Enter your domain name' and a blue button labeled 'SCAN' is positioned in the center.

<https://www.cookiepro.com/products/cookie-consent/>



The screenshot shows the OneTrust website. The top navigation includes 'CCPA', 'Products', 'Solutions', 'Customers', and 'Services'. The main heading is 'Cookie Consent and Website Scanning' in white text on a dark background. Below it, there is a sub-heading: 'GDPR and ePrivacy Compliance for Cookies & Online Tracking Technologies'. The main content area features a grid of six dark blue boxes with white text and icons, highlighting key features: 'Used By 75,000 Websites', '50 Supported Languages', '6M Pre-Categorized Cookies', '7 Years in Production', 'Highly Scalable Billions of Impressions', and 'GDPR, IAB & ePrivacy Compliant'.











<https://www.onetrust.com/products/cookies/>



The screenshot shows the Termly website. The top navigation includes 'Products', 'Resources', 'Pricing', 'US', and 'Sign In'. The main heading is 'GDPR Cookie Consent Manager' in large black text. Below it, there is a paragraph: 'Use our all-in-one cookie consent tool to create a cookie policy, build a GDPR cookie banner, and manage user consent. Try for free today!'. A blue button labeled 'Start Building Cookie Consent' is positioned below the paragraph. On the right side, there is a grid of six white boxes with icons and labels for various services: 'Google Analytics', 'Google Ads', 'Cookie Law', 'GDPR', 'App Store', and 'AdSense'.

<https://termly.io/products/cookie-consent-manager/>

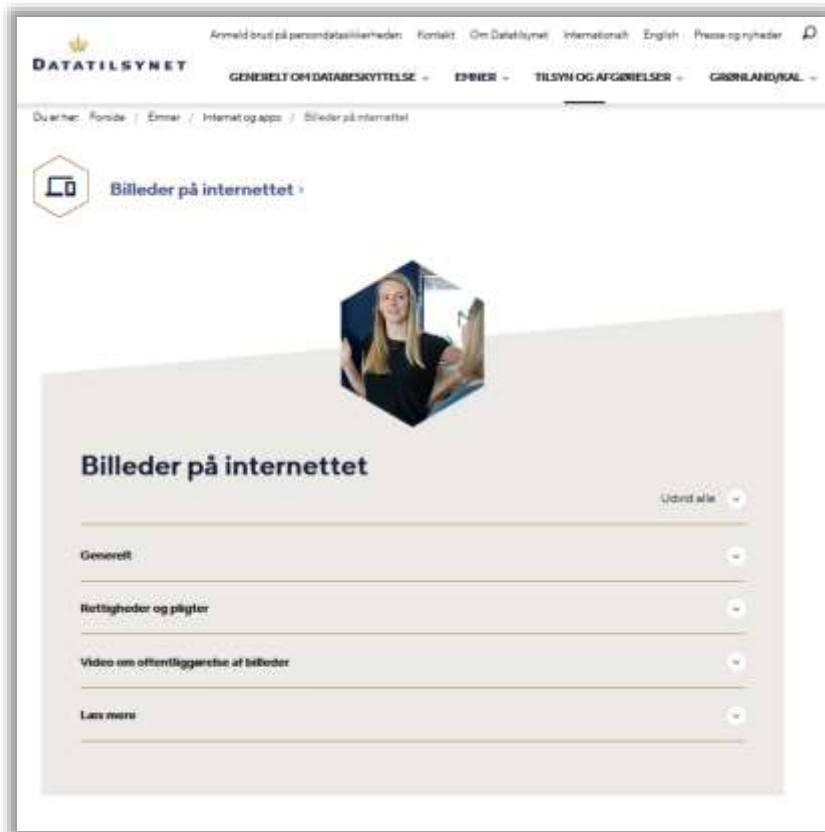
## Анализ порочной практики мобильных приложений по сбору данных пользователей

App	Summary of findings
 Clue	Sends birth year to <b>Amplitude</b> , <b>Apptimize</b> , and <b>Braze</b> . Sends Advertising ID to <b>Adjust</b> , <b>Amplitude</b> , and <b>Facebook</b> .
 Grindr	Sends GPS coordinates to <b>AdColony</b> , <b>Braze</b> , <b>Bucksense</b> , <b>MoPub</b> , <b>OpenX</b> , <b>Smaato</b> , <b>PubNative</b> , <b>Vungle</b> , and others. Sends the IP address to <b>AppNexus</b> and <b>Bucksense</b> , and information about "relationship type" to <b>Braze</b> . Sends Advertising ID to all of these third parties and others, except <b>Braze</b> .
 Happn	Sends country, gender and age segment of the user to <b>Google</b> . Sends Advertising ID to <b>Adjust</b> and <b>Facebook</b> .
 Muslim: Qibla Finder	Sends IP address to <b>Appodeal</b> . Sends Advertising ID to <b>AppLovin</b> , <b>Appodeal</b> , <b>Facebook</b> , and <b>Liftoff</b> .
 My days	Sends GPS coordinates and Wi-Fi access point information to <b>Neura</b> , <b>Placed</b> , and <b>Placer</b> . Sends IP address and a list of installed apps on the phone to <b>Placed</b> . Sends Advertising ID to <b>AppLovin</b> , <b>Liftoff</b> , <b>Google</b> , <b>Ogury Presage</b> , and <b>Placed</b> .
 My Talking Tom 2	Sends IP address to <b>Mobfox</b> , <b>PubNative</b> , and <b>Rubicon Project</b> . Sends Advertising ID to <b>AppsFlyer</b> , <b>AppLovin</b> , <b>Facebook</b> , <b>IQzone</b> , <b>ironSource</b> , <b>Mobfox</b> , <b>Outfit7</b> , and <b>Rubicon Project</b> .
 OkCupid	Sends GPS coordinates and answers to personal questions to <b>Braze</b> . Sends detailed device information to <b>AppsFlyer</b> . Sends Advertising ID to <b>AppsFlyer</b> , <b>Facebook</b> and <b>Kochava</b> .
 Perfect365	Sends various location data such as GPS coordinates and Wi-Fi access point information to <b>Fysical</b> , <b>Safegraph</b> , and <b>Vungle</b> . Sends GPS coordinates unencrypted to <b>Receptiv</b> . Sends Advertising ID to <b>Amazon</b> , <b>Chocolate</b> , <b>Facebook</b> , <b>Fluxloop</b> , <b>Fyber</b> , <b>Fysical</b> , <b>InMobi</b> , <b>Inner-Active</b> , <b>Ogury Presage</b> , <b>Safegraph</b> , <b>Receptiv</b> , <b>Unacast</b> , <b>Unity3d</b> , and <b>Vungle</b> .
 Tinder	Sends GPS position and "target gender" to <b>AppsFlyer</b> and <b>LeanPlum</b> . Sends Advertising ID to <b>AppsFlyer</b> , <b>Branch</b> , <b>Facebook</b> , and <b>Salesforce (KruX)</b> .
 Wave Keyboard	Sends Advertising ID to <b>Crashlytics</b> , <b>Facebook</b> , <b>Flurry</b> , <b>OneSignal</b> .

Норвежский Совет Потребителей (Forbrukerrådet) 14.01.2020 опубликовал аналитический отчет "Out of control. How consumers are exploited by the online advertising industry", в котором описывается порочная практика десятка приложений (Tinder, Grindr, OkCupid, Perfect365, MyDays и т.д.) по сбору персональных данных своих пользователей информацию, включая точное местоположение, сексуальную ориентацию, религиозные и политические убеждения, сведения об употреблении наркотиков и другую информацию, и под дальнейшей передаче собранных сведений в распоряжение по крайней мере 135 различных сторонних компаний.



## Разъяснение от Datatilsynet об обработке персональных данных при публикации фото людей в Интернете



Датский надзорный орган Datatilsynet пересмотрел свои разъяснения от 2002 года относительно обработки персональных данных при публикации фото людей в Интернете на основании оценки того, является ли это ситуационным изображением или портретным изображением. Цель ситуационных фотоизображений - это действие или ситуация, например фотографии зрителей для концерта. Цель портретных фотоизображений - изобразить одного или нескольких конкретных лиц.

Разграничение между ситуативными и портретными изображениями на практике оказалось нечетким, а технологическое и социальное развитие с 2002 года привело к значительному изменению в использовании Интернета. Так, фотографии опознаваемых лиц сегодня широко публикуются на веб-сайтах и в социальных сетях, таких как Facebook и Instagram.

На этом фоне Датское агентство по защите данных решило изменить свою практику и больше не проводить различие между ситуативными и портретными изображениями, а далее – оценивать вопрос о публикации фотографии субъекта данных (без его согласия) в Интернете на основании всесторонней оценки изображения и цели публикации.

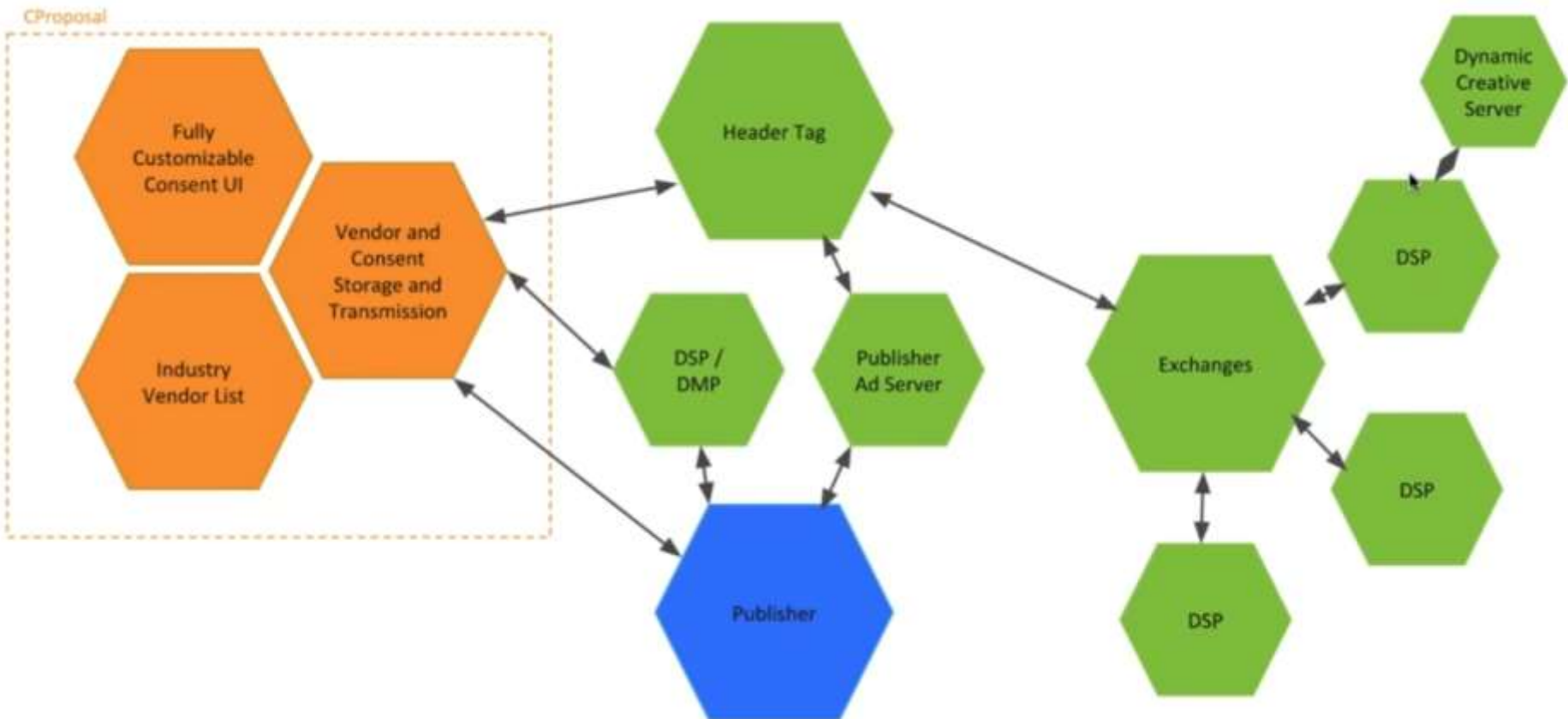
## Руководство ENISA по конфиденциальности и защите данных в мобильных приложениях



GDPR PRINCIPLES	INDICATIVE PRIVACY RISKS	INDICATIVE REQUIREMENTS
Lawfulness, fairness and transparency Art.5(1)(a)	Unlawful, excessive and incorrect processing (e.g. due to permissions to unauthorised parties to access personal data through the app).	<p>App providers/developers should make sure that they have a legal basis for the processing of personal data.</p> <p>App providers/developers should inform the data subjects properly about their data processing activities. This may help the users to understand what personal data is collected by them and why.</p> <p>App providers/developers should be aware of data subject rights such as rights to access, rectification, erasure, data portability. They should implement appropriate processes to support these rights.</p>
Purpose limitation Art.5(1)(b)	Excessive collection and sharing of data (e.g. due to multiple sensors of mobile devices that are activated without need).	App providers/developers should use the data for a specific purpose that the data subjects have been made aware of and no other, without further consent. If the personal data is used for purposes other than the initial, they should be anonymised or the data subjects must be notified and their consent must be re-obtained.
Data minimisation Art.5(1)(c)	Excessive processing (e.g. due to use of third party libraries).	The minimum amount of data for specific processing should be processed by app providers/developers. For instance, they should not store the exact location point when a generic location area is sufficient for their app functionalities.
Accuracy Art.5(1)(d)	Outdated data pose identity theft risks.	Rectification processes into data management should be embedded in the app design.
Storage limitation Art.5(1)(e)	Undue data disclosure (e.g. due to cloud storage services used by mobile app developers).	Personal data must not be stored longer than necessary. App providers/developers should provide the "right to be forgotten" to the data subjects. This data must be kept only for a certain period of time for non-active users.
Integrity and confidentiality Art.5(1)(f)	Unlawful data processing, data loss, data breach, data destruction or damage	App providers/developers should ensure that the security requirements of the personal data and the processing systems are met. This encompasses integrity and confidentiality as well as availability and resilience (Art. 35(1)(b) GDPR). For instance, the appropriate control access mechanisms should be embedded into the apps infrastructure in order to detect or monitor unauthorized access to the data.

## 347 Transparency and Consent Framework от IAB Europe

Бюро интерактивной рекламы Европы (консорциум, включающий Google и другие компании), совместно с IAB Tech Lab, разработало технический протокол, известный как Transparency and Consent Framework (TCF), для обеспечения надлежащего получения согласий пользователей для обработки их данных в целях рекламы и аналитики. Данный механизм предназначен для использования владельцами рекламных площадок (издателей), вендоров, рекламодателей и рекламных агентств, платформ управления контентом (Consent Management Platforms).





16.05.2023 Бюро интерактивной рекламы (IAB) Europe запустило Transparency & Consent Framework (TCF) V2.2, который стал ответом на план действий, утвержденный Бельгийским управлением по защите данных (Belgian DPA). Являясь добровольным стандартом и инструментом отчетности для издателей, продавцов и платформ управления согласиями в сфере цифровой рекламы, TCF призван облегчить выполнение определенных положений GDPR и Директивы ePrivacy.

Среди прочих изменений, новая версия TCF включает пересмотренные названия и описания целей обработки данных, новые сроки хранения для всех целей, исключение законного интереса для рекламы и персонализации контента, введение категорий данных, используемых в сочетании с целями, и более надежную программу соответствия требованиям поставщиков.

Технологические платформы управления согласиями (CMPs) и участники рекламного рынка, подчиняющиеся правилам IAB, с 30 сентября 2023 года будут обязаны (см. Приложение А здесь) запрашивать отдельное согласие в тех случаях, когда они захотят создавать или поддерживать индивидуальный цифровой профиль пользователя для персонализации рекламы или контента. Предыдущая версия Руководства допускала обработку персональных данных для этих целей на основании обозначенного пользователю законного интереса оператора.

# Анализ Авторiteit Persoonsgegevens соответствия сервисов видеоконференций требованиям приватности



AUTORITEIT  
PERSOONSGEGEVENS

Home Corona Over privacy ▾ Onderwerpen ▾ Zelf doen

## Keuzehulp privacy bij videobel-apps

Nieuwsbericht / 15 april 2020

Categorie:

Privacy & corona,

Veilig thuiswerken tijdens corona, Apps

De Autoriteit Persoonsgegevens (AP) heeft bij 13 veelgebruikte videobel-apps gekeken naar de belangrijkste privacyaspecten. Zoals welke gegevens de app verzamelt, wat de app daarmee doet en of de communicatie beveiligd is. De AP krijgt namelijk veel vragen over privacy bij zulke apps, nu mensen massaal zijn gaan videobellen tijdens de coronacrisis. Daarom biedt de AP een keuzehulp om verschillende videobel-apps te vergelijken.

Let op: de AP heeft geen uitgebreid, technisch onderzoek kunnen doen naar de apps. De AP gaat af op wat bedrijven zelf zeggen over wat hun videobel-apps met uw gegevens doen, bijvoorbeeld in hun privacyverklaring.

### Keuzehulp videobellen

Welke app u het beste kunt gebruiken, hangt ten eerste af van wat u ermee wilt. Bijvoorbeeld of u een gesprek wilt voeren met één of met meerdere personen.

## Privacy Decision-making aid: Video Call Apps

As of 15 April 2020

UNOFFICIAL TRANSLATION by Christopher Schrick, CIPR/ECIP/CIPT/CISA

	Zoom	GoTo	Microsoft Teams	Skype	WhatsApp	Signal	Jitsi	Zoom	GoTo	Microsoft Teams	Skype	WhatsApp	Signal	Jitsi
<b>What does the app offer?</b>														
(group chat (text))														
1-to-1 calls (audio and/or video)														
group calls (audio and/or video)														
set up and manage yourself (self-hosted)														
participation in conversation w/o creating an account														
use in browser														
use on different platforms (cross-platform)														
<b>What data does the app collect?</b>														
address book														
location data														
call data														
metadata														
linking data with data from other products or profiles														
<b>For what purposes does the app process data?</b>														
For using the app														
For improving the app														
Show (personalised) advertisements														
<b>How does the information look like?</b>														
Data Processing Agreement: possible														
Data transfer to 3rd parties (if so, what data and to whom)														
Location of data controller														
data remain in the Netherlands														
data remain in the EU														
<b>Is the communication secure?</b>														
end-to-end encryption (even the provider of the app cannot access the content of the communication)														
encryption of traffic during transfer, so that third parties cannot access it (even the provider of the app may be able to access it, but this does not mean it will happen)														
minimisation of metadata use														
encryption by default														
everyone can check source code (open source)														
<b>How does the app make money?</b>														
paid subscription or paid version														
(personalised) advertisements														
donations														
otherwise														
<b>Where can you find information?</b>														
privacy statement (link to the Dutch version / in readable form)														
privacy statement in Dutch														

1. Video only
2. After each session
3. Complete file name
4. Steps for getting Microsoft Edge or Google Chrome
5. Not for video in a call
6. Avoid using Google Chrome
7. Microsoft Edge
8. Not for file transfer
9. Please make sure you are in a secure location
10. Only for desktop
11. Not for file transfer
12. Not for file transfer
13. Not for file transfer
14. Not for file transfer
15. Not for file transfer
16. Not for file transfer
17. Not for file transfer
18. Not for file transfer
19. Not for file transfer
20. Not for file transfer
21. Not for file transfer
22. Not for file transfer
23. Not for file transfer
24. Not for file transfer
25. Not for file transfer
26. Not for file transfer
27. Not for file transfer
28. Not for file transfer
29. Not for file transfer
30. Not for file transfer
31. Not for file transfer
32. Not for file transfer
33. Not for file transfer
34. Not for file transfer
35. Not for file transfer
36. Not for file transfer
37. Not for file transfer
38. Not for file transfer
39. Not for file transfer
40. Not for file transfer
41. Not for file transfer
42. Not for file transfer
43. Not for file transfer
44. Not for file transfer
45. Not for file transfer
46. Not for file transfer
47. Not for file transfer
48. Not for file transfer
49. Not for file transfer
50. Not for file transfer
51. Not for file transfer
52. Not for file transfer
53. Not for file transfer
54. Not for file transfer
55. Not for file transfer
56. Not for file transfer
57. Not for file transfer
58. Not for file transfer
59. Not for file transfer
60. Not for file transfer
61. Not for file transfer
62. Not for file transfer
63. Not for file transfer
64. Not for file transfer
65. Not for file transfer
66. Not for file transfer
67. Not for file transfer
68. Not for file transfer
69. Not for file transfer
70. Not for file transfer
71. Not for file transfer
72. Not for file transfer
73. Not for file transfer
74. Not for file transfer
75. Not for file transfer
76. Not for file transfer
77. Not for file transfer
78. Not for file transfer
79. Not for file transfer
80. Not for file transfer
81. Not for file transfer
82. Not for file transfer
83. Not for file transfer
84. Not for file transfer
85. Not for file transfer
86. Not for file transfer
87. Not for file transfer
88. Not for file transfer
89. Not for file transfer
90. Not for file transfer
91. Not for file transfer
92. Not for file transfer
93. Not for file transfer
94. Not for file transfer
95. Not for file transfer
96. Not for file transfer
97. Not for file transfer
98. Not for file transfer
99. Not for file transfer
100. Not for file transfer

<https://autoriteitpersoonsgegevens.nl/nl/nieuws/keuzehulp-privacy-bij-videobel-apps>

<https://workupload.com/file/8FzuCsSkMky>

<b>CONTENTS</b>	
<b>BACKGROUND</b>	03
<b>ABOUT THE RESEARCH</b>	05
<b>WHY GETTING PRIVACY RIGHT MATTERS</b>	09
"Social pressure" to care about privacy	10
People need reassurance through honesty and clarity	11
<b>THE KEY FINDINGS</b>	
<b>1 MAKE IT MEANINGFUL</b>	12
What is meaningful marketing?	12
The value exchange	13
Privacy/value trade-offs	13
Clearly communicating value	15
Relevant and timely messages	16
<b>2 MAKE IT MEMORABLE</b>	18
Prioritise conscious data sharing	20
Remind people of their choices	20
<b>3 MAKE IT MANAGEABLE</b>	23
The "say-do" gap	24
Reaching the digital marketing sceptics	25
<b>KNOW BETTER, DO BETTER</b>	28
In summary	28
Establish the basics	29
Go beyond the basics	31
Final thoughts	32
<b>APPENDIX</b>	33
Personalised Services Study: Automating the Consumer Experience	33
Data Privacy Study: Consumer Model of Data Privacy	34
Data Ethics Study: Data Ethics and Effectiveness	35
Personalised Services Deep Dive	36
Data Privacy Deep Dive	38
Responsible Marketing Deep Dive	39

Исследование 2021г. показывает, что люди готовы делиться своими данными, если они доверяют компании. Чтобы завоевать доверие нужно превышать ожидания своих пользователей и придерживаться трех простых правил.

### **Вкладывать в маркетинг смысл:**

- людям комфортнее делиться данными, если они понимают зачем они это делают;
- реклама более ценна, если она соответствует интересам человека;
- момент демонстрации рекламы и контекст максимально важны;
- понимайте своих клиентов, чтобы соответствовать их интересам и предоставлять им правильные контексты наполненные нужной им ценностью и смыслом.

### **Делать запоминающийся маркетинг:**

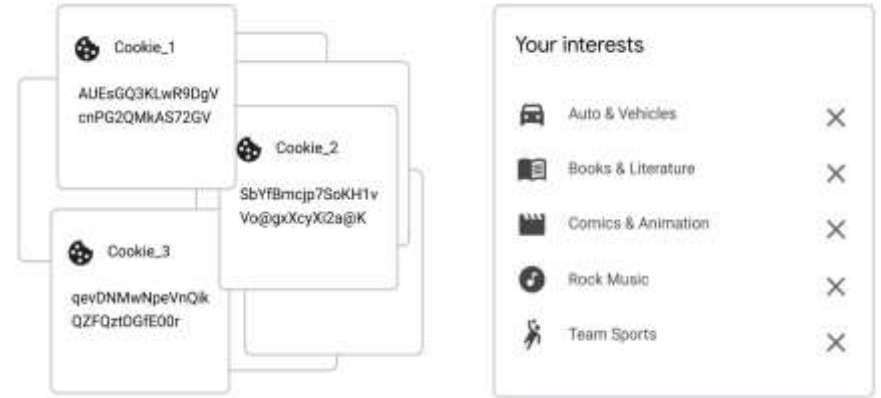
- клиенты хотят помнить, как, зачем и для чего они предоставили данные (неожиданные звонки/смс/е-мейлы не радуют никого);
- 8 из 10 опрошенных считают, что компаниям нужно давать больше информации о данных, которые они обрабатывают;
- если клиент помнит как он оставлял свои данные, то он/она воспринимает увиденную рекламу более позитивно;
- порой клиенту нужно напоминать как и когда он/она дал согласие для рекламных целей.

### **Сделать маркетинг управляемым для пользователя:**

люди хотят чувствовать контроль над своими данными;  
некоторые люди более охотно настраивают свои предпочтения если чувствуют, что они могут управлять своими данными.

## Таргетинг по интересам: Google представил очередную альтернативу cookies – технология Topics

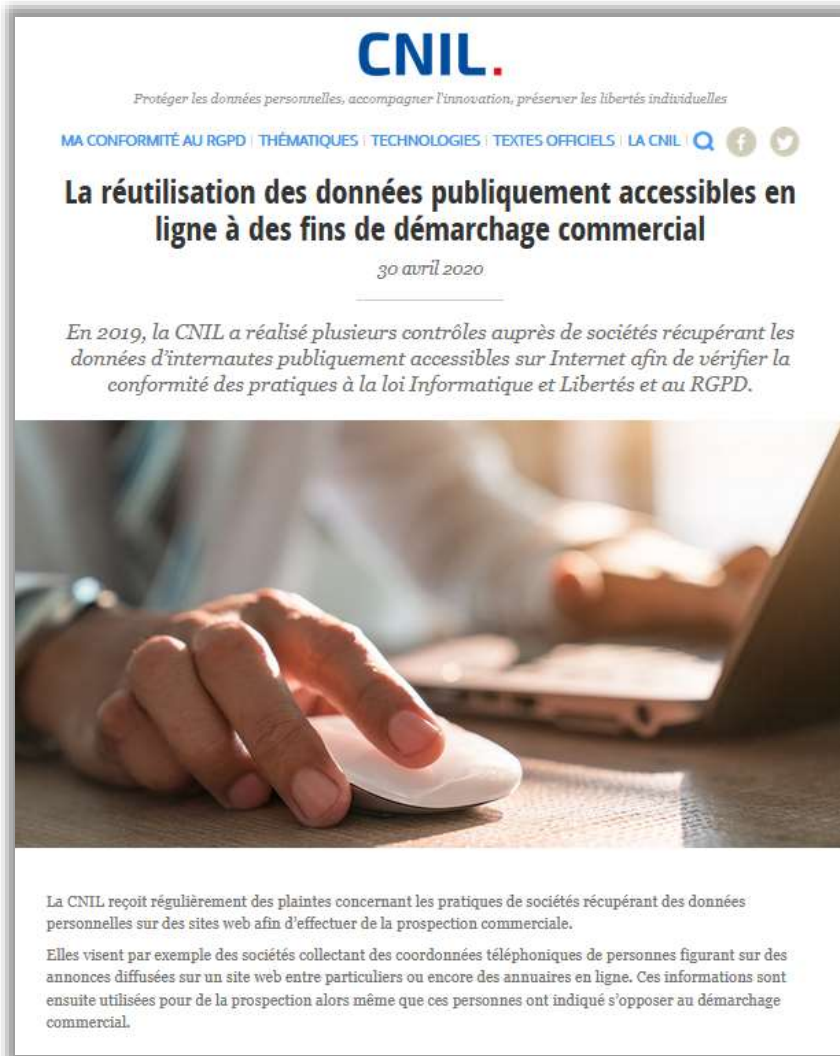
Google протестировал технологию федеративного обучения на основе когорт – FLoC (Federated Learning of Cohorts), получил обратную связь и решил, что необходимо разработать новое решение. Очередная альтернатива cookies получила название Topics, поскольку определяет интересы пользователя. Topics, как и FLoC, является частью инициативы Privacy Sandbox, направленной на улучшение ситуации с безопасностью данных. Браузер Chrome будет определять интересы на основе истории посещения сайтов за неделю. Информация будет храниться в течение трех недель, при этом старые «топики» автоматически удаляются. В процессе не будут задействованы внешние серверы, в том числе Google, все данные сохранятся исключительно на устройстве пользователя.



Когда человек зайдет на сайт, участвующий в программе, Topics выберет три темы (одну на каждую неделю) — например, фитнес, путешествия и автомобили — и поделится этой информацией с площадкой и ее рекламными партнерами. Google обещает, что пользователь сможет контролировать этот механизм — просматривать категории интересов, удалять те, которые ему не нравятся, либо вообще отключать эту опцию.

Поскольку данные обрабатываются на уровне браузера, Topics является более прозрачным механизмом по сравнению со сторонними cookies и другими видами рекламной «слежки», уверяет корпорация. Бизнесу, который имеет «на руках» информацию об интересах потребителя, не понадобятся скрытые техники вроде фингерпринтинга для показа релевантной рекламы. В Google заявляют, что вскоре разработчики, владельцы сайтов и рекламодатели смогут протестировать новую технологию. К проекту планируют привлечь внешних партнеров, в первую очередь для классификации и систематизации интересов. Многие детали API (объем классификатора, сколько «топиков» будет подсчитано за неделю, количество категорий, предоставляемых партнерам по каждому запросу) будут финализировать с учетом обратной связи от участников экосистемы. Пока предполагается, что API раздаст «ярлыки» сайтам, которые посещает пользователь. Затем браузер определит наиболее частотные и поделится этой информацией с площадками, где размещается реклама. Таким образом, пользователю покажут релевантные объявления и никто не узнает, на какие конкретно ресурсы он заходил. Список интересов из примерно 350 категорий будет публичным. Со своей стороны, Chrome гарантирует отсутствие «чувствительных» тем вроде пола, религии, сексуальной ориентации. Появление Topics означает, что Google прекратит работу над FLoC.

## Руководство CNIL о повторном использовании общедоступных данных для прямого маркетинга



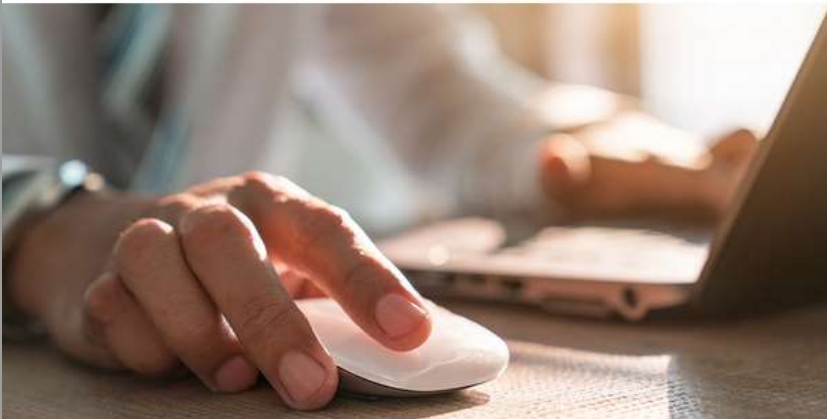
**CNIL.**  
*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL 🔍 🌐 📄

### La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial

30 avril 2020

*En 2019, la CNIL a réalisé plusieurs contrôles auprès de sociétés récupérant les données d'internautes publiquement accessibles sur Internet afin de vérifier la conformité des pratiques à la loi Informatique et Libertés et au RGPD.*



La CNIL reçoit régulièrement des plaintes concernant les pratiques de sociétés récupérant des données personnelles sur des sites web afin d'effectuer de la prospection commerciale.

Elles visent par exemple des sociétés collectant des coordonnées téléphoniques de personnes figurant sur des annonces diffusées sur un site web entre particuliers ou encore des annuaires en ligne. Ces informations sont ensuite utilisées pour de la prospection alors même que ces personnes ont indiqué s'opposer au démarchage commercial.

Французский орган по защите данных (CNIL) опубликовал 30 апреля 2020 года руководство в отношении повторного использования общедоступных персональных данных, в частности опубликованных на веб-сайтах контактных данных субъектов, для целей прямого маркетинга. Такие персональные данные не могут быть повторно использованы для осуществления прямых маркетинговых контактов с помощью электронной почты или иных средств связи без предварительного согласия субъектов и их информирования об источниках получения данных. Также необходимо уважать право субъектов данных на возражение. Компании, использующие сервисы веб-скрейпинга, должны, среди прочего, проверять характер и источник получаемых таким образом персональных данных, соблюдать принцип минимизации обрабатываемых данных, информировать субъектов об обработке их данных, надлежащим образом оформлять договорные отношения с сервис-провайдерами и проводить оценку воздействия на защиту данных (DPIA), если это необходимо.



## Руководство датского Datatilsynet о защите данных в прямом маркетинге



Датский орган по защите данных (Datatilsynet) опубликовал 30.06.2023 новое руководство по обработке персональных данных в контексте прямого маркетинга.

В руководстве рассматриваются следующие вопросы:

- правила обработки персональных данных; описание маркетинговых мероприятий;
- типы персональных данных, которые должны использоваться;
- использование данных о детях;
- типичные примеры маркетинговой деятельности;
- телемаркетинг и электронный маркетинг;
- профилирование и автоматизированные решения;
- правовые основания для обработки данных.

## Руководство Берлинского надзорного органа об обработке данных при рекламной деятельности



Orientierungshilfe der Aufsichtsbehörden  
zur Verarbeitung von personenbezogenen Daten  
für Zwecke der Direktwerbung  
unter Geltung der Datenschutz-Grundverordnung (DS-GVO)<sup>1</sup>

**Redaktion:**

Bayerisches Landesamt für Datenschutzaufsicht  
Promenade 18, 91522 Ansbach  
E-Mail: [poststelle@lda.bayern.de](mailto:poststelle@lda.bayern.de)  
Web: [www.lda.bayern.de](http://www.lda.bayern.de)  
Tel.: 0981/180093 0  
Fax: 0981/180093 800

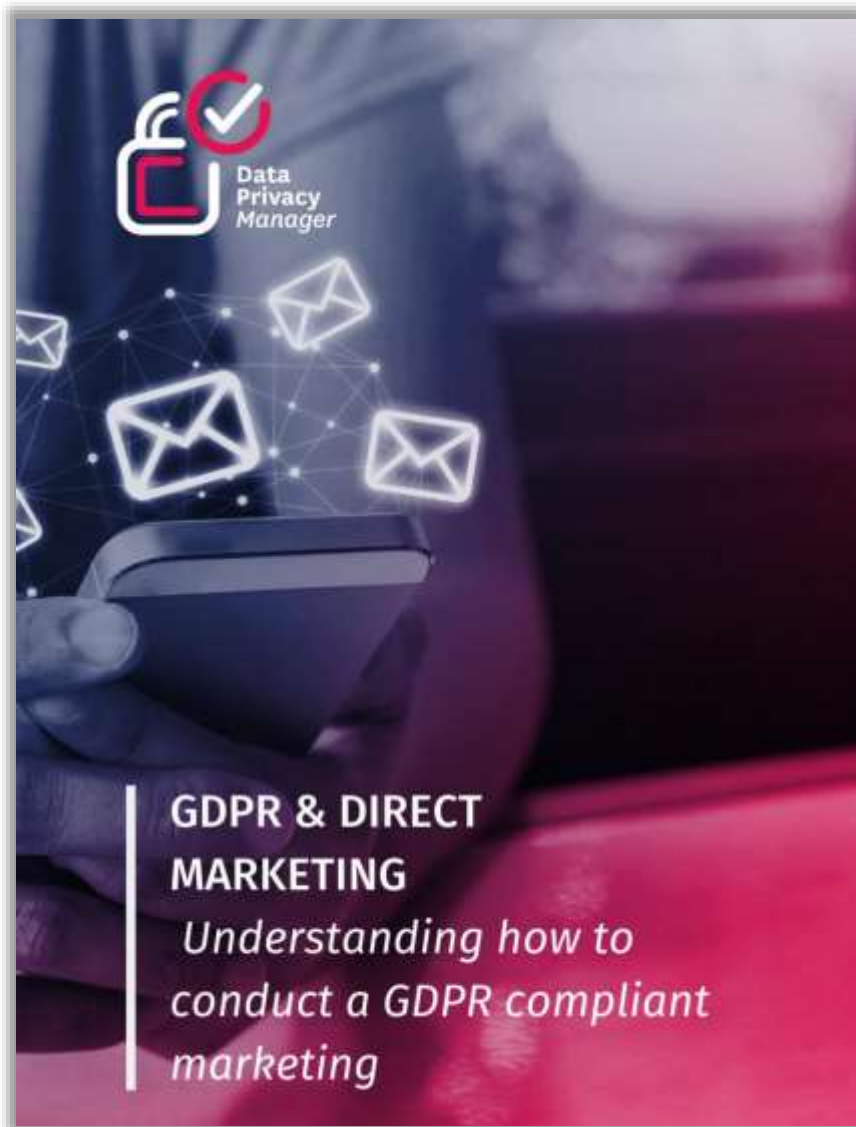
**Stand:**

Februar 2022

<sup>1</sup> Diese Orientierungshilfe thematisiert nicht das Thema Adresshandel, da hierzu gesonderte Beratungen erfolgen werden.

Берлинский орган по защите данных 16.06.2022 опубликовал руководство об обработке данных при рекламной деятельности, в котором указаны законные основания, на которые маркетинговые компании могут опираться при обработке персональных данных, а также соответствующие права, о которых субъекты данных должны быть проинформированы.

Кроме того, руководство содержит образцы писем, которые субъекты данных могут использовать для обращения в компании и реализации своих прав, а также дополнительную информацию, направленную на помощь субъектам данных в отстаивании своих прав в контексте рекламы.



1. GDPR and Direct Marketing.....	1
2. Marketing challenges.....	2
2.1. What is considered Direct Marketing.....	3
2.2. What is not considered Direct Marketing.....	5
3. Requirements for compliant Marketing.....	5
3.1. The difference between Directive and Regulation.....	6
3.2. GDPR requirements.....	6
3.2.1. Lawfulness, fairness, and transparency.....	7
3.2.2. Purpose limitation.....	11
3.2.3. Adequate, limited and relevant processing (data minimization).....	11
3.2.4. Accuracy principle.....	13
3.2.5. Storage limitation.....	13
3.2.6. Technical and organizational measures (Integrity and confidentiality principle).....	14
3.2.7. Data subjects' rights fulfillment.....	15
3.3. ePrivacy Directive requirements.....	16
3.3.1. Cookies under the ePrivacy.....	17
4. E-mail marketing.....	18
4.1. Sending e-mails to your existing customers.....	19
4.2. B2B Marketing communication.....	20
4.3. Marketing opt-out.....	21
4.4. Disclosing information.....	23
5. Telemarketing.....	23
6. Targeted website advertising.....	24
6.1. Who is a data controller?.....	25
7. Location-based marketing.....	26
7.1. The obligation of the data controller when using location data.....	27
8. Exporting data outside the EEA.....	27
9. Conclusion.....	28
10. About Data Privacy Manager.....	29
DISCLAIMER.....	30

## 356 6 правил реализации функции «пригласить друга»

When you implement the «invite a friend» feature, you should take into account that the user's friends (non-users) are personal data subjects. Therefore, you need to have any legal grounds for their personal data processing. However, it is reasonable to assume that you cannot obtain consent from non-users, and your legitimate interest doesn't prevail over the interest of non-users. Because of this, you are not likely to get a consent or concluded contract with non-users and it is very difficult to demonstrate that legitimate interests applies.

You should remember all GDPR principles, especially the "data minimization" principle: **don't process personal data if something can be done without personal data processing.**

- ☑ Do not collect non-user's personal data unless "invite a friend" feature cannot be implemented without the personal data collection.
- ☑ An invitation is better to send via the user's messengers or an e-mail without your intermediary as a data controller, if possible. You may only create an invitation in an appropriate format.
- ☑ Do not send an invitation directly from you and on behalf of you because you do not have any legal grounds for non-user's personal data processing.
- ☑ Do not add advertising in the invitation send by user, since you need to have a freely given and an explicit consent from non-users for advertising.
- ☑ Access to non-users data is strictly limited by the term and the number of the involved non-users. Do not store non-user's personal data longer than it is necessary for sending an invitation. It is applicable only in case when "invite a friend" feature cannot be made without the storage. You shall realize the "search and delete" approach.
- ☑ Do not establish relations between the current users in your customer database and invited friends by default, whereas it will be additional personal data. This can be established when you suggest a loyalty program, and the relations are necessary to consider invited friends.

## Нижнесаксонский LfD Niedersachsen о законности запроса даты рождения в интернет-магазинах



Ведомство по защите данных Нижней Саксонии (LfD Niedersachsen) 20.03.2024 опубликовало пресс-релиз о завершении судебного разбирательства в Высшем административном суде Нижней Саксонии по поводу использования даты рождения в качестве обязательного поля в интернет-магазинах. LfD Niedersachsen отметило, что судебное решение последовало за предписанием LfD Niedersachsen о прекращении и запрете деятельности одной из онлайн-аптек за использование даты рождения в процессе оформления заказа, независимо от типа заказываемого товара.

Обработка данных о дате рождения не может быть основана на договорной необходимости, юридическом обязательстве или законных интересах, однако законные интересы могут быть применимы в случае невыполнения обязательств по оплате; и если согласие является единственным применимым правовым основанием, поле ввода в форме должно быть четко обозначено как "добровольное", а клиентам должна быть предоставлена возможность продолжить процесс заказа без ввода данных.

На онлайн-аптеки по-прежнему распространяются вышеупомянутые выводы, учитывая, что исключения, предусмотренные специальными положениями о рецептах на лекарства, применимы не ко всем товарам, продаваемым аптеками.

<https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/geburtsdatum-als-pflichtfeld-in-webshops-oft-rechtswidrig-230666.html>

<https://voris.wolterskluwer-online.de/browse/document/22d96b5b-998b-412a-a7e7-18fd741383cb>

## Руководство британского ICO по правомерному осуществлению прямого маркетинга

### Guidance on direct marketing



#### [Direct marketing guidance](#)

This is the ICO's main direct marketing guidance. It sets out the main things to consider or do when you want to do direct marketing activities. It takes you through the steps you are likely to go through.



#### [The Guide to PECR](#)

This tells you what you need to know if you want to send electronic marketing messages (by phone, email and text), or if you want to use cookies or similar for online advertising. It also contains detailed guidance if you want to know more.



#### [Direct marketing: Guide for SMEs](#)

This is a simple list for small organisations who plan to use direct marketing.



#### [Business-to-business marketing](#)

If you want to send marketing to other businesses this guidance will help you to comply.



#### [Direct marketing and the public sector](#)

This guidance helps public authorities understand when their promotions might count as direct marketing.



#### [Guidance for the use of personal data in political campaigning](#)

This guidance provides clarity and practical advice to help those processing personal data in political campaigning to comply with the law.



#### [Organisations using marketing services of data brokers](#)

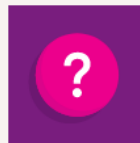
If you are thinking about using the marketing services of data brokers this guidance helps you understand what you'll need to do to comply.

### Practical direct marketing resources



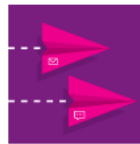
#### [Direct marketing checklist](#)

A step-by-step guide through the process of using information for direct marketing purposes.



#### [Direct marketing FAQs](#)

Frequently asked questions for small organisations, including small businesses, small charities and sole traders.



#### [Sending direct marketing messages: At-a-glance guide](#)

A simple guide to the rules on sending direct marketing by phone call, electronic mail (email and text), fax and post.



#### [Sending direct marketing: Choosing your lawful basis](#)

A simple table listing methods of sending direct marketing along with what the PECR requirements are and what your choice of lawful basis is likely to be if you are using people's information.



#### [Data protection self assessment: Direct marketing](#)

Assess your business in the area of direct marketing in line with the PECR and data protection legislation.



#### [Training resources for your business: PECR](#)

A training module providing information about what to do if you want to reach your customers through electronic marketing. It also looks at the use of cookies.

## Руководство британского ICO по использованию soft opt-in для электронных маркетинговых коммуникаций

Управление комиссара по информации ("ICO") 01.11.2022 опубликовало заявление об использовании организациями «мягкого согласия» (soft opt-in) для отправки электронных маркетинговых сообщений своим клиентам. Использование такой практики должно сопровождаться выполнением пяти требований:

1. контактные данные должны быть получены непосредственно от человека, которому организация хочет отправить маркетинговую рассылку, что означает, что soft opt-in доступен только для одной организации, которая первоначально собрала контактные данные;
2. контактные данные должны быть получены в ходе продажи или переговоров о продаже, примерами последних являются подписка на бесплатную пробную версию, запрос предложения или дополнительной информации о продуктах/услугах, что должно включать форму явного сообщения со стороны заинтересованного лица;
3. электронные маркетинговые сообщения касаются аналогичных продуктов или услуг организации, при этом ключевым моментом является то, может ли заинтересованное лицо обоснованно ожидать прямой маркетинг конкретного продукта или услуги от данной организации, т.е. soft opt-in не будет применяться к рассылке маркетинговых сообщений других организаций;
4. организация предоставила заинтересованному лицу возможность отказаться от рассылки в момент сбора данных простым способом, а простое размещение отказа в политике конфиденциальности организации будет недостаточным;
5. организация предоставляет заинтересованному лицу возможность отказаться или отказаться от услуг в каждом последующем сообщении простым и понятным способом.

ICO также подготовило подробное руководство по использованию организациями soft opt-in, которое включает четкие примеры хорошей и плохой практики.



Итальянский орган по защите данных (Garante) 18.03.2024 объявил о вступлении в силу Кодекса поведения и соответствующего органа контроля. Кодекс поведения регулирует деятельность по телепродажам и телемаркетингу и направлен на защиту пользователей от нежелательных звонков. Контрольный орган отвечает требованиям, изложенным в правилах защиты частной жизни, и включает в себя достаточный уровень компетентности, а также независимость и беспристрастность, чтобы он мог контролировать применение Кодекса поведения.

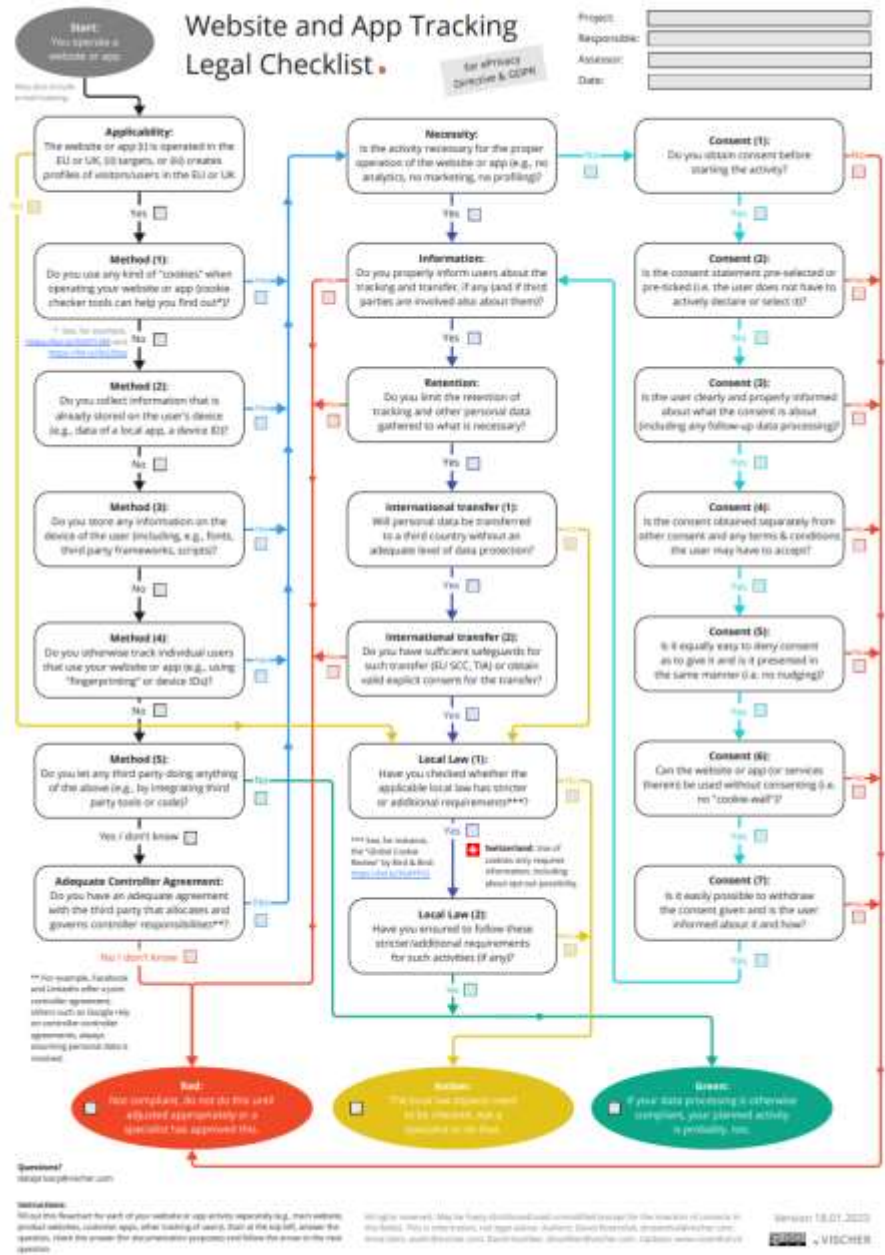
Компании, соблюдающие Кодекс поведения, должны принимать специальные меры, гарантирующие правильность и законность действий по обработке данных, осуществляемых в процессе телемаркетинга, в том числе необходимо:

- собирать конкретное согласие для индивидуальных целей;
- точно информировать людей, с которыми связываются, об использовании их данных;
- проводить оценку воздействия в случае использования автоматизированной обработки;
- обеспечивать полное осуществление прав, предусмотренных законодательством о неприкосновенности частной жизни.

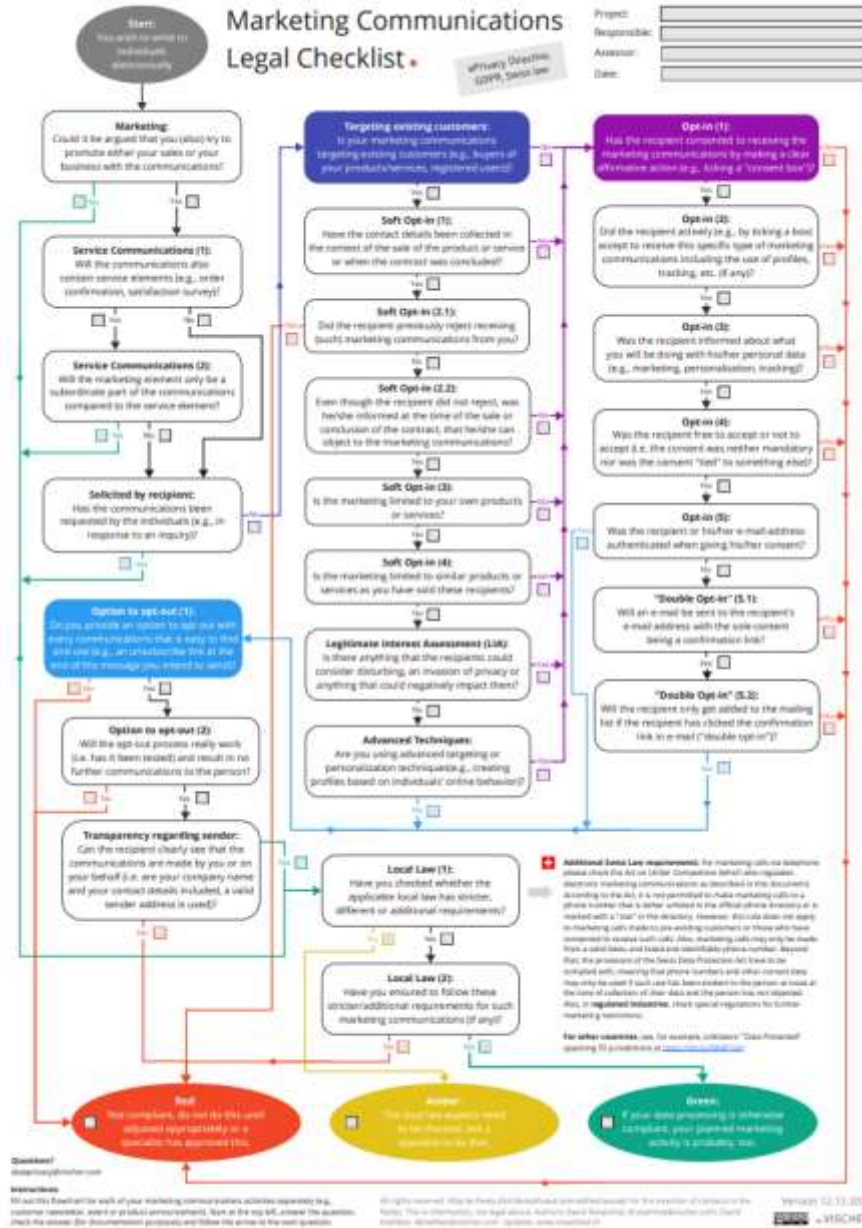
Кодекс поведения также предусматривает штраф за каждый договор, заключенный в результате контакта, на который не было получено надлежащего согласия.



# 361 Чек-лист по правомерному мониторингу на сайтах и мобильных приложениях

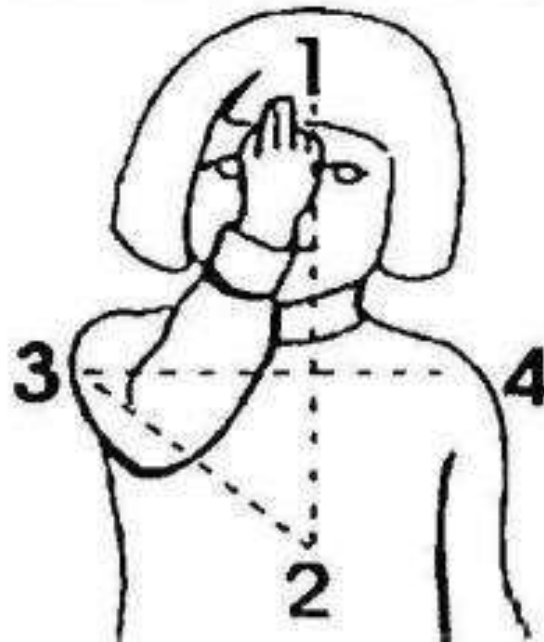


# 362 Чек-лист по правомерному осуществлению прямого маркетинга

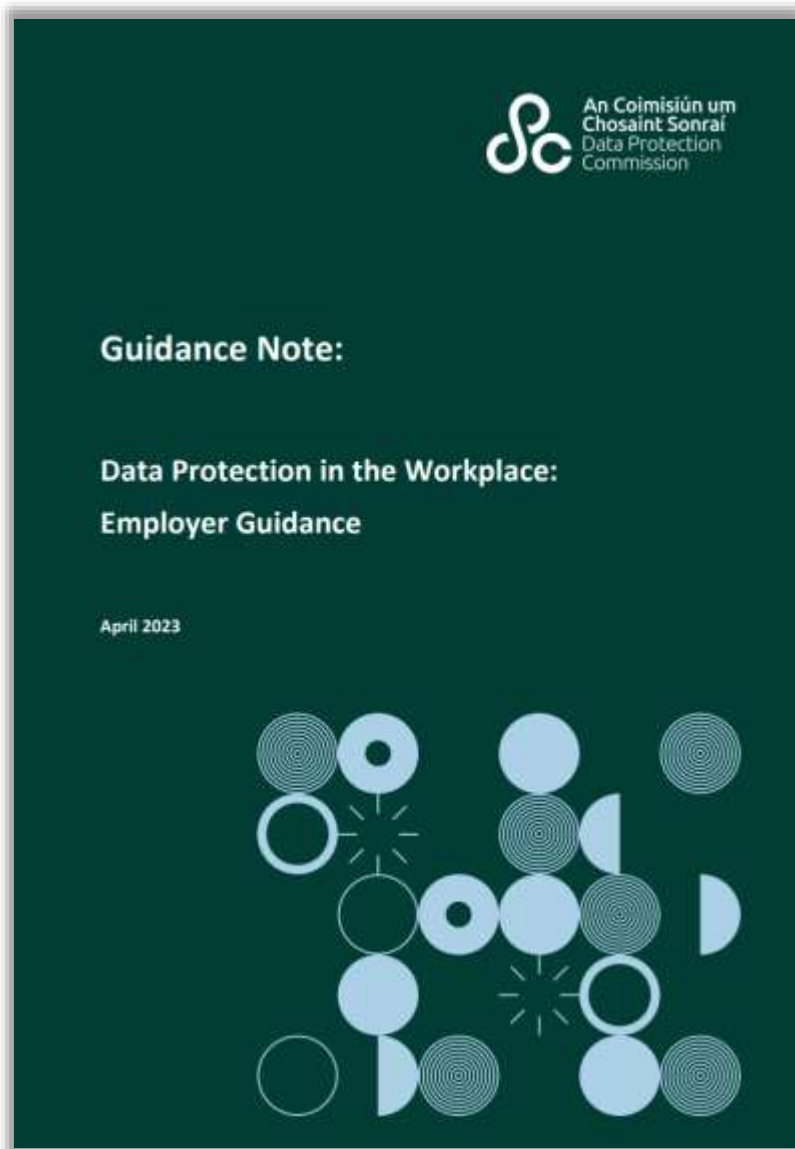


# Обработка данных персонала и соискателей

## 4 EASY STEPS FOR GDPR COMPLIANCE



## 364 Руководство ирландской DPC по защите данных на рабочем месте



Комиссия по защите данных Ирландии ("DPC") 28.04.2023 выпустила руководство для работодателей по защите данных на рабочем месте. Руководство направлено на оказание помощи работодателям как контролерам данных в отношении их обязательств и обязанностей при обработке персональных данных своих сотрудников, бывших сотрудников и потенциальных работников. В руководстве приводятся примеры, демонстрирующие, могут ли календарь Outlook и должностная инструкция быть классифицированы как источники персональных данных.

## Руководство шведского Datainspektionen по обработке персональных данных в трудовых правоотношениях



The screenshot shows the website of the Swedish Data Protection Authority (Datainspektionen). The main heading is "Behandling av personuppgifter i arbetslivet". Below the heading is a sub-heading: "Här kan du läsa om hur personuppgifter i arbetslivet får behandlas enligt dataskyddsförordningen. Informationen vänder sig i första hand till arbetsgivare inom både privat och offentlig sektor. Den kan också vara till hjälp för arbetstagare, arbets sökande, fackförbund och branschorganisationer." Below this are seven topic boxes: "När gäller dataskyddsförordningen?", "Arbetsgivarens personuppgiftsansvar", "Tillåten behandling – vilka krav gäller?", "Rekryteringssystem och kompetensdatabaser", "Kontroll och övervakning av anställda", "Biometri", and "Tillsyn, sanktionsavgifter och skadestånd".

**Behandling av personuppgifter i arbetslivet**

Här kan du läsa om hur personuppgifter i arbetslivet får behandlas enligt dataskyddsförordningen. Informationen vänder sig i första hand till arbetsgivare inom både privat och offentlig sektor. Den kan också vara till hjälp för arbetstagare, arbets sökande, fackförbund och branschorganisationer.

- När gäller dataskyddsförordningen?
- Arbetsgivarens personuppgiftsansvar
- Tillåten behandling – vilka krav gäller?
- Rekryteringssystem och kompetensdatabaser
- Kontroll och övervakning av anställda
- Biometri
- Tillsyn, sanktionsavgifter och skadestånd

Шведский орган по защите данных (Datainspektionen) опубликовал 5 октября 2020 года обновленное руководство по трудоустройству и защите данных. Руководство дает информацию о том, как работодатели могут обрабатывать персональные данные о своих работниках, какие правила следует соблюдать при приеме на работу, каковы ограничения по контролю и мониторингу работников, а также по обработке биометрии.

## Руководство датского Datatilsynet по защите данных в трудовых отношениях



Датский орган по защите данных ("Datatilsynet") 29.03.2023 обновил свое руководство по защите данных в контексте трудовых отношений. После последнего пересмотра руководства в декабре 2020 года он обновил его в свете последних практик, в том числе в отношении получения справок о судимости и рекомендаций. Datatilsynet разъяснил ряд разделов руководства, включая раздел об обязанности работодателя предоставлять информацию и о раскрытии персональных данных. Структура руководства также была скорректирована, чтобы сделать его более легким для чтения и более полезным.

<https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/mar/datatilsynets-vejledning-om-databeskyttelse-i-ansættelsesforhold-er-revideret>

<https://www.datatilsynet.dk/Media/0/8/Vejledning%20om%20databeskyttelse%20i%20forbindelse%20med%20ans%C3%A6ttelsesforhold.pdf>

## Руководство CNIL по обработке и защите персональных данных при дистанционном режиме работы

**CNIL.**  
*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

MES DÉMARCHES | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL

### Salariés en télétravail : quelles sont les bonnes pratiques à suivre ?

12 mai 2020

*La pandémie du coronavirus (COVID-19) a incité de nombreuses entreprises à mettre en place des solutions de télétravail. Si vous êtes concerné(e)s par ce type de dispositif, vous devez suivre quelques règles pour garantir votre propre sécurité et celle de votre entreprise.*

- Suivez les instructions de votre employeur
- Sécurisez votre connexion internet
- Favorisez l'usage d'équipements fournis et contrôlés par votre entreprise
- Si vous devez utiliser un ordinateur personnel, assurez-vous qu'il est suffisamment sécurisé
- Si vous devez utiliser votre téléphone personnel, protégez vos données et limitez les accès
- Communiquez en toute sécurité
- Soyez particulièrement vigilant sur les tentatives d'hameçonnage

Французский орган по защите данных (CNIL) 12.05.2020 выпустил руководство по обработке и защите персональных данных при дистанционном режиме работы. В руководстве затронуты вопросы использования оборудования, поставляемого работодателем, защиты служебных персональных компьютеров и иных устройств с помощью шифрования, а также использования систем видеоконференций, прошедших сертификацию и обеспечивающих приватность пользователей.

## Руководство норвежского Datatilsynet по обработке данных при проверке благонадежности соискателей



**Datatilsynet**

### Før ansettelse - bakgrunnsundersøkelser

I rekrutteringsprosessen kan arbeidsgiveren ha behov for å undersøke arbeidssøkerne nærmere ved å samle inn mer informasjon om dem enn det som står i søknadene. Slik informasjon handler om de enkelte kandidatene og regnes som personopplysninger.

#### Innhold

1. Innledning
2. Kredittvurdering
3. Polititattest
4. Integritetsundersøkelser («Integrity Due Diligence»)

Skriv ut alt innholdet

Søk i dette innholdet

Sist endret: 11.03.2022

#### Innledning

Arbeidsgiveren må følge de generelle reglene i *personvernforordningen* når personopplysninger behandles. Det er her verdt å merke seg plikten til å:

- [gi informasjon om behandlingen](#) til arbeidssøkerne,
- [legge til rette for arbeidssøkernes rettigheter](#),
- [slette opplysningene](#), og
- ha tilfredsstillende [informasjonsikkerhet og internkontroll](#).

[Les mer om virksomhetenes plikter](#)

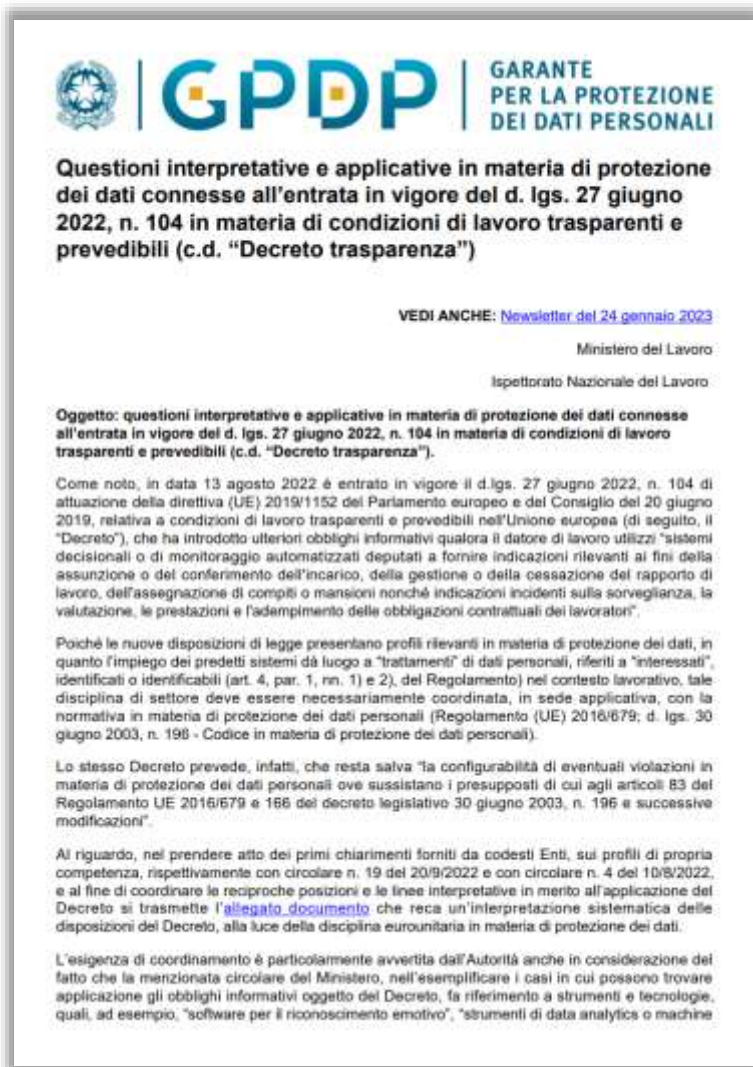
I denne veiledningen ser vi nærmere på når arbeidsgiveren kan gjennomføre ulike former for bakgrunnsjekk, og hvilke særlige plikter som gjelder. Vi ser på:

- Innhenting av *kredittvurdering*,
- Innhenting av *polititattest*
- såkalte *integritetsundersøkelser* («Integrity Due Diligence-undersøkelser»).

Норвежский орган по защите данных («Datatilsynet») 28.03.2022г. опубликовал руководство по обработке персональных данных при проверке благонадежности соискателей ("background checks") на замещение вакантных должностей, которая включает в себя управление связанными с соискателями юридическими, репутационными и комплаенс (предотвращение и урегулирование возможного или существующего конфликта интересов, противодействие коррупции) рисками, а также проверку полноты и достоверности предоставленных соискателями сведений. Текст руководства доступен только на норвежском языке.



## Руководство итальянского Garante по обеспечению прозрачности мониторинга и автоматизации в контексте трудовых отношений



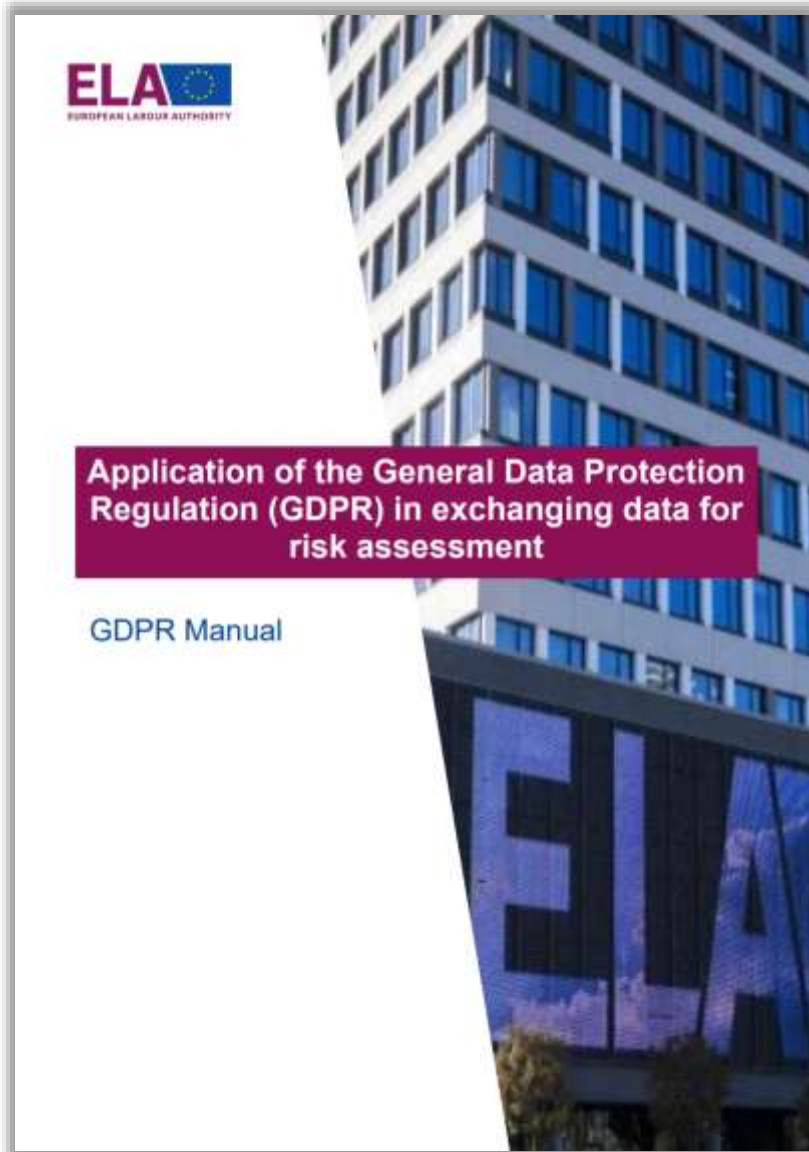
Итальянский орган по защите данных ("Гаранте") 24.01.2023 опубликовал руководство по интерпретации защиты данных и вопросам правоприменения, связанным с Законодательным декретом № 104 от 27.06.2022 ("Декрет о прозрачности").

Декрет о прозрачности, который применяется к трудовым договорам и другим формам занятости, ввел, среди прочего, обязанность работодателей надлежащим образом информировать работников, если они используют автоматизированные системы принятия решений или мониторинга для целей найма или назначения, или для другой деятельности, связанной с трудовыми отношениями и их управлением.

Работники должны иметь возможность знать основные параметры, используемые для программирования или обучения автоматизированных систем, включая механизмы оценки эффективности, а также надежность и кибербезопасность систем. Кроме того, эти информационные обязательства не заменяют собой обязательства, уже предусмотренные GDPR. Внедрение систем мониторинга в рабочем контексте всегда должно быть предметом предварительной проверки работодателем условий законности, установленных правилами дистанционного управления, а также оценки рисков для проверки их влияния на права и свободы соответствующих лиц.

В отношении особо инвазивных систем, таких как инструменты машинного обучения, рейтинга и ранжирования, их использование создает критические вопросы с точки зрения соразмерности и рискует вступить в противоречие с принципами защиты данных и национальными отраслевыми правилами, защищающими свободу, достоинство и частную жизнь работников.

# Руководство ELA по применению GDPR для оценке рисков при обмене данными в контексте трудовых отношений



<b>1.0 Introduction</b> .....	<b>6</b>
1.1 Brief history of data protection law .....	7
1.2 Legal framework .....	7
<b>2.0 Basic concepts and principles of data protection</b> .....	<b>9</b>
2.1 What is personal data and what is not? .....	9
2.2 What is processing? .....	11
2.3 Basic principles .....	12
2.4 Legal bases .....	16
<b>3.0 Data protection actors</b> .....	<b>20</b>
3.1 Data subject .....	20
3.2 Controller .....	20
3.3 Processor .....	21
3.4 Data Protection Officer (DPO) .....	22
3.5 Data Protection Authority (DPA) .....	23
<b>4.0 Rights of data subjects</b> .....	<b>25</b>
4.1 Transparency .....	25
4.2 Rights of data subjects .....	26
4.3 Restricting data subject rights .....	30
<b>5.0 Check list</b> .....	<b>31</b>
<b>Annex I: Fictional case study</b> .....	<b>32</b>
<b>Annex II: Further reading</b> .....	<b>35</b>

## Позиция LfD Niedersachsen в отношении обработки данных работников в связи с болезнью



Орган по защите данных Нижней Саксонии ("LfD Niedersachsen") в декабре 2022 года заявил свою позицию об обработке данных в связи с предоставлением работниками листов нетрудоспособности и продолжением оплаты их труда в случае болезни. В рамках процедуры оценки для определения нетрудоспособности и продолжения выплаты вознаграждения работодатели участвуют в обработке персональных данных работников в соответствии с GDPR, включая обработку контактных данных работников, данных медицинского страхования и специальных категорий персональных данных.

LfD Niedersachsen сформировал обзор требований по защите данных, которые должны соблюдаться в рамках вышеупомянутой процедуры оценки, в частности:

- ◇ правовые основания для частных и государственных органов, обрабатывающих данные работников;
- ◇ разрешение доступа к персональным данным работников;
- ◇ передача данных между больничными кассами и работодателем;
- ◇ получение справок о нетрудоспособности;
- ◇ технические и организационные меры для обработки данных о здоровье;
- ◇ указания по применению вышеописанных правил на практике.

## Руководство французского CNIL для рекрутеров в отношении обработки персональных данных соискателей

Nature des obligations	Article RGPD	RT	ST	co-RT
Rédiger un écrit précisant les obligations respectives de chacun des acteurs	26, 28	✓	✓	✓
Désigner un représentant au sein de l'Union européenne (pour les responsables de traitement et les sous-traitants situés hors de l'Union européenne)	27	✓	✓	✓
Documenter les instructions du responsable de traitement concernant les traitements de données par le sous-traitant	0	✓	✓	✓
Obtenir et conserver une autorisation écrite préalable du responsable de traitement pour recourir aux services d'un sous-traitant	28	✗	✓	✗
Tenir un registre conforme aux exigences de l'article 30 du RGPD	30	✓	✓	✓
Réaliser une analyse d'impact relative à la protection des données (si les conditions en sont réunies). Pour plus d'informations sur l'analyse d'impact, voir la fiche n° 10 de ce guide.	35	✓	Le contrat passé entre le ST et le RT prévoit notamment que le ST aide le RT à garantir le respect de ses obligations en matière d'AIPD, compte tenu de la nature du traitement et des informations dont il dispose	✓
Organiser une information spécifique des co-contractants (responsable de traitement, sous-traitant, responsable conjoint de traitement) en cas de violation du RGPD	28	✗	✓	✗
Informar la CNIL et les personnes concernées (principalement les candidats) en cas de violation des données, si les conditions sont réunies	33-34	✓	✗	✓
Fournir aux personnes concernées les informations obligatoires	12 à 14	✓	Le ST doit parfois en fonction de la nature du traitement et des mesures organisationnelles retenues aider le RT à s'acquitter de son obligation d'informer les personnes concernées, dans les conditions fixées par le contrat passé avec le RT.	✓
Traiter les demandes d'exercice de droits (accès, effacement, opposition, etc.)	15 à 23	✓	✗	✓
Assister le responsable de traitement dans le traitement de telles demandes	28	Sans objet	✓	Sans objet

Французский орган по защите данных ("CNIL") 30.01.2023 опубликовал руководство для рекрутеров в отношении обработки персональных данных соискателей, которое состоит из трех частей:

- ◇ описание основных требований GDPR к защите персональных данных в сфере подбора персонала;
- ◇ вопросы и ответы по использованию новых технологий рекрутерами и по конкретным вопросам, например, связанным с дискриминацией;
- ◇ представление о передовых практиках, которые следует применять для обеспечения соответствия требованиям GDPR.

# Итальянское руководство по использованию электронной почты и Интернета в контексте трудоустройства



# GPDP

GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context - 1 March 2007 [1408680]

[doc. web n. 1408680]

### Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context - 1 March 2007

#### The Garante per la protezione dei dati personali

Having convened today, with the participation of Prof. Francesco Pizzetti, President, Mr. Giuseppe Chiaravalloti, Vice-President, Mr. Giuseppe Fortunato and Mr. Mauro Paissan, Members, and Mr. Giovanni Buttarelli, Secretary General;

Having regard to the claims, reports and questions submitted with regard to the processing of personal data by employers in connection with the use by employees of IT and computerised tools;

Having regard to the records on file;

Having regard to sections 24 and 154(1), letter b) and c) of the Personal Data Protection Code (legislative decree no. 196 of 30 June 2003);

Having regard to the considerations made by the Secretary General in pursuance of article 15 of the Garante's Rules of Procedure no. 1/2000;

Acting on the report submitted by Mr. Mauro Paissan;

#### Whereas

### 1. Use of E-Mail and the Internet in the Employment Context

#### 1.1. Foreword

The analysis of several claims, reports and questions pointed to the need for laying down some measures as necessary and/or appropriate in order to ensure that the processing of personal data performed by employers to verify that e-mails and the Internet are used appropriately in the employment context is brought fully into line with the legislation in force.

There are a few basic assumptions to make:

- a. employers are responsible for ensuring that employees are provided with workable IT tools and use them appropriately, by setting out the respective usage guidelines in the employment context also in the light of trade union laws and rights;
- b. employers are required to take suitable security measures to ensure integrity and availability of information systems and data, also in view of preventing misuse and the liability possibly arising therefrom (sections 15, 31 et seq., 167, and 169 of the Code);

- c. it is increasingly necessary to protect the employees concerned, partly because use of the devices in question – which are already quite common in the employment context – is bound to be enhanced at a fast pace in many activities also performed outside the workplace;
- d. indeed, use of the Internet by employees may be analysed, profiled and tracked in full by processing browsing log files as collected, for instance, by a proxy server and/or another data storage device. E-mail services are also liable to controls – based for instance on the keeping of traffic log files and the storage of e-mail messages – that might ultimately enable the employer (i.e. the data controller) to become apprised of the contents of such correspondence;
- e. the information in question contains personal data, including sensitive data, related to employees and/or third parties, whether identified or identifiable. <sup>(1)</sup>

#### 1.2. Protecting Employees

The personal data at issue may concern, in addition to work-related information, the private life and/or personal sphere of both employees and third parties. As pointed out by the European Human Rights Court, the line between these two areas is at times difficult to draw. <sup>(2)</sup>

The workplace is a community where it is necessary to ensure that data subjects' rights, fundamental freedoms, and dignity are protected. To that end, employees must be enabled to freely express their own personalities within the framework of mutual rights and duties; additionally, they are entitled to a reasonable protection of their privacy in personal and professional relationships alike (Articles 2 and 41(2) of the Italian Constitution; section 2087 of the Civil Code; see also section 2(5) of the Digital Administration Code (legislative decree no. 82 of 7 March 2005) as for the right to have the processing of data by electronic networks brought into line with respect for fundamental rights and freedoms and data subjects' dignity). <sup>(3)</sup>

It is no mere chance that several employers – in organising their work and the necessary tools – have envisaged usage mechanisms whereby ad-hoc working areas have been made available to take strictly personal notes, given the increasing amount of network-based activities and the availability of new flat-rate schemes; alternatively, they have allowed reasonable use to be made of IT tools for private purposes.

### 2. Personal Data Protection Code and Sector-Related Legislation

#### 2.1. General Principles

In issuing the guidelines below, the Garante is taking account of the right to personal data protection, the need for the processing to be regulated by affording a high level of protection to individuals, and the principles of simplification, harmonisation, and effectiveness set out in sections 1 and 2 of the data protection Code. These guidelines are subject to adjustments in the light of the experience gathered and technological innovations.


#### 2.2. Sector-Related Legislation

Some sector-related rules that are left unprejudiced by the data protection Code provide for specific prohibitions and/or limitations – such as those laid down by the Workers' Statute in respect of distance monitoring (sections 113, 114, and 184(3) of the Code; sections 4 and 8 of Act no. 300/1970).

Data protection legislation must be applied jointly with sector-related rules concerning employer-employee relationships and the use of technologies in such sectors, where data protection legislation is either left unprejudiced or expressly referred to (see section 47(3), letter b), of the Digital Administration Code). <sup>(4)</sup>

#### 2.3. Principles Set out in the Data Protection Code

## Руководство итальянского Garante по обработке метаданных в корпоративной электронной почте



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

**Provvedimento del 21 dicembre 2023 - Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" [9978728]**

VEDI ANCHE [Newsletter del 6 febbraio 2024](#)  
[doc. web n. 9978728]

Provvedimento del 21 dicembre 2023 - Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati"

Registro dei provvedimenti  
n. 642 del 21 dicembre 2023

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzone, presidente, la prof.ssa Ginevra Carrina Feroni, vicepresidente, l'avv. Guido Scorza, componente e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito, "Regolamento"), con particolare riguardo agli artt. 5, 6 e 88 dello stesso;

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali", recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito "Codice"), con particolare riguardo agli artt. 113 e 114 dello stesso;

VISTI gli artt. 4 e 8 della l. 20 maggio 1970, n. 300, nonché l'art. 10 del d.lgs. 10 settembre 2003, n. 276;

CONSIDERATO che nell'ambito di accertamenti condotti dal Garante con riguardo ai trattamenti di dati personali effettuati nel contesto lavorativo è emerso il rischio che programmi e servizi informatici per la gestione della posta elettronica, commercializzati da fornitori in modalità cloud, possano raccogliere, per impostazione predefinita, in modo preventivo e generalizzato, i metadati relativi all'utilizzo degli account di posta elettronica in uso ai dipendenti (ad esempio, giorno, ora, mittente, destinatario, oggetto e dimensione dell'email), conservando gli stessi per un esteso arco temporale; ciò talvolta ponendo, altresì, limitazioni al cliente (datore di lavoro) in ordine alla possibilità di modificare le impostazioni di base del programma informatico al fine di disabilitare la

Итальянский орган по защите данных (Garante) опубликовал 06.02.2024 руководящий документ относительно обработки персональных данных, осуществляемой в контексте работы, и риска сбора по умолчанию метаданных, связанных с использованием учетных записей электронной почты сотрудниками и сохранением таких данных.

В руководящем документе рекомендуется государственным и частным учреждениям тщательно проверять, позволяют ли используемые ИТ-программы и службы управления электронной почтой работодателю изменять базовые настройки, чтобы предотвратить сбор метаданных, или ограничить срок хранения семью днями.

## 375 Итальянский Кодекс поведения для работодателей



Итальянский орган по защите данных (Garante) утвердил 14.02.2024 Кодекс поведения, представленный Национальной ассоциацией агентств по трудоустройству (Assolavoro).

Кодекс поведения определяет лучшие практики надлежащей обработки данных соискателей. Организации, соблюдающие Кодекс поведения, должны обрабатывать только те данные, которые строго необходимы для установления трудовых отношений. Организациям, соблюдающим Кодекс поведения, запрещено выяснять политические, религиозные или профсоюзные взгляды соискателей. Кодекс поведения указывает, что работодатели не должны проводить предварительный отбор по семейному положению, беременности или инвалидности даже с согласия человека.

К другим запрещенным действиям, согласно Кодексу поведения, относятся:

- получение информации из непрофессиональных социальных каналов;
- получение профессиональных рекомендаций соискателя от предыдущих работодателей без предварительного прямого согласия;
- обработка информации, связанной с дисциплинарными нарушениями или судебными разбирательствами, даже с согласия человека.

Кодекс поведения требует проведения оценки воздействия (DPIA) и предоставления работникам информации о механизмах автоматизации и периодической оценки. В случае автоматизированной обработки необходимо гарантировать работникам право на вмешательство человека, выражение своего мнения и оспаривание решения.



◇ 24.05.2023 Управление комиссара по информации (ICO) опубликовало новое руководство по реагированию на запросы субъектов доступа к данным (DSARs) для работодателей. Право доступа дает субъектам данных право запрашивать копию своих персональных данных у организаций, если отказ в ответе будет равносителен правонарушению.

◇ Руководство охватывает несколько вопросов, связанных с DSARs, с практическими примерами для работодателей, включая информацию о следующем:

- что такое право доступа и обязательства контролеров в этой связи в соответствии с законодательством о защите данных;

- формат DSARs;

- обращение за разъяснениями по поводу DSARs;

- случаи, когда утаивание информации является оправданным;

- специфика раскрытия информации о правонарушениях в сообщениях о доносительстве;

- DSARs в контексте сотрудников, подписавших соглашения о неразглашении или мировые соглашения;

- DSAR в контексте дисциплинарных процессов или рассмотрения жалоб.

◇ Руководство охватывает аспекты DSAR, которые работодатели должны оценивать в отношении:

- раскрытия сведений об электронной почте, в которую копируются сообщения работников;

- раскрытие информации в социальных сетях работодателя;

- идентификации и защиты интересов третьих сторон.



## Руководство британского ICO по обработке данных персонала с фокусом на его мониторинг

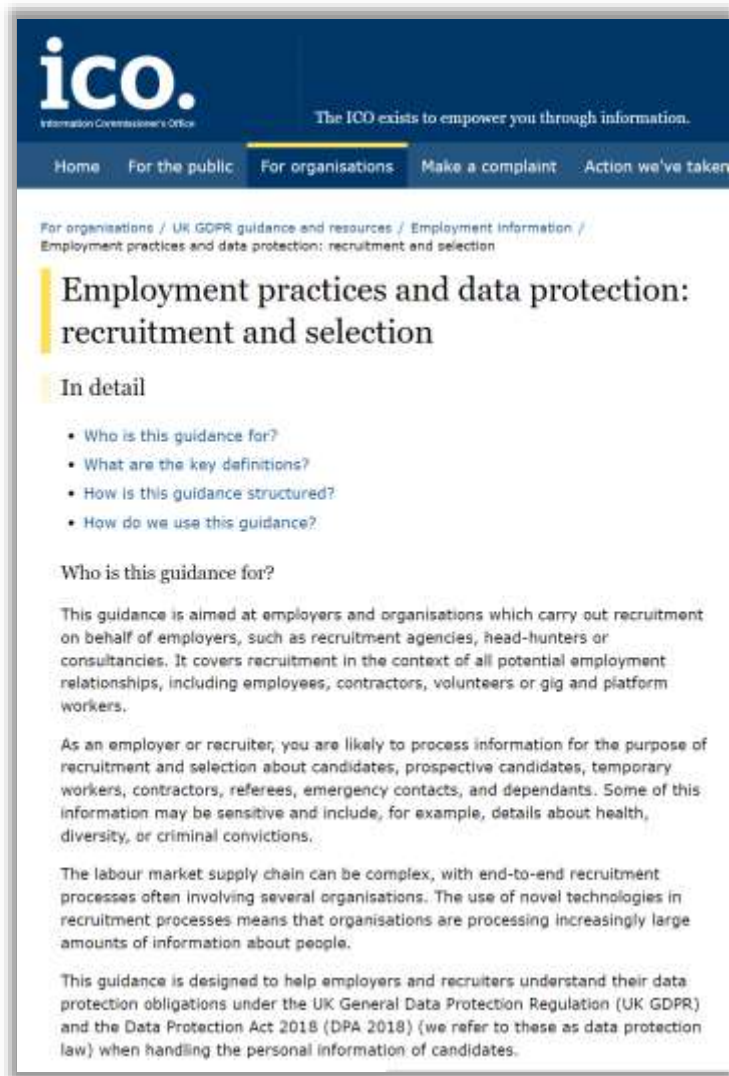


Руководство опубликовано 03.10.2023 и предназначено для работодателей и призвано обеспечить большую нормативную определенность, защитить права работников на защиту данных, а также помочь работодателям укрепить доверие к работникам, клиентам и пользователям услуг. Кроме того, руководство содержит практические рекомендации, которые помогут работодателям соответствовать Общему положению о защите данных Великобритании (UK GDPR) и Закону о защите данных 2018 года (DPA 2018).

Если организация намерена осуществлять наблюдение за работниками, то, согласно руководству, она должна предпринять определенные шаги, в том числе:

- иметь четко определенную цель и использовать для ее достижения наименее интрузивные средства;
- наличие законных оснований для обработки данных работников, таких как согласие или юридическое обязательство;
- проведение оценки воздействия на защиту данных (DPIA) для любого мониторинга, который может привести к высокому риску для прав работников;
- информирование работников о характере, масштабах и причинах мониторинга;
- информирование работников о проводимом мониторинге в доступной для понимания форме;
- хранить только ту информацию, которая имеет отношение к делу;
- предоставление личной информации, собранной в ходе мониторинга, работникам, если они подают запрос на доступ к ней.

## 378 Руководство британского ICO по подбору и найму персонала



The screenshot shows the ICO website page for 'Employment practices and data protection: recruitment and selection'. The page header includes the ICO logo and the tagline 'The ICO exists to empower you through information.' The navigation menu includes 'Home', 'For the public', 'For organisations', 'Make a complaint', and 'Action we've taken'. The breadcrumb trail is 'For organisations / UK GDPR guidance and resources / Employment information / Employment practices and data protection: recruitment and selection'. The main heading is 'Employment practices and data protection: recruitment and selection'. Below the heading is a section 'In detail' with a list of bullet points: 'Who is this guidance for?', 'What are the key definitions?', 'How is this guidance structured?', and 'How do we use this guidance?'. The 'Who is this guidance for?' section contains three paragraphs of text explaining the scope and purpose of the guidance.

Управление комиссара по информации (ICO) опубликовало 12.12.2023 руководство по подбору и найму персонала.

Руководство призвано помочь работодателям и рекрутерам понять свои обязательства по защите данных при работе с персональными данными кандидатов.

Проект руководства должен:

- помочь обеспечить большую нормативную определенность;
- защитить права кандидатов на защиту данных;
- помочь работодателям и рекрутерам проводить эффективную работу по подбору персонала в соответствии с законами о защите данных.

## Руководство латвийского DVI по обработке персональных данных в рамках трудовых обязанностей с помощью информационных систем

#DViskaidro: Darba pienākumu ietvaros iegūto personas datu izmantošana. Informācijas sistēmas

Atskaidrojot tēstus

Publiskums: 12.03.2024.

**"Atbilstošs mērķis datu apstrādei NAV:**

- ziņkārība;
- fakts, ka informācija ir pieejama;
- atziēbība vai cita veida kaitniecība."

saka Valdis Dombrovskis, kurš ilgus gadus ir strādājis medicīnas nozarē.

Lasītāji profesijā un nozarē mēs strādājam, veicot savu darba pienākumu, mūsu darbā tieši vai netieši varam rīkoties citu personu - kolēģu, līdzstrādnieku, klientu - datiem. Lai arī šai informācijai varam piekļūt un to varam apstrādāt dažādos veidos, pirms tam būtu jānodrošinā - vai tas, ko ar datiem plānot darīt, būs loģiski?

Šajā skaidrojamā koncentrēsimies uz datu apstrādi, izmantojot informācijas sistēmas un datubāzes, kurās ir personu dati un kurām piekļuve tiek piešķirta darba tiesiskā atbilstību vai (Atbilstēta ietvaros).

Vidējais informācijas sistēmas un datubāzes (turpmāk - Sistēmas), kas satur personas datus un kurām ir piekļuve nodarbinotājiem, ir valsts nozarēs informācijas sistēmas, piemēram, Fizisko personu reģistrs, klientu darījumības - komercdarbības ietvaros, tomēr jāpatur prātā arī organizāciju iekšējās sistēmas, kurās parasti tiek glabāti klientu iestāžu un t.c. saņemtie dokumenti.

Parasti organizācija (vai arī citas gadījumos - normatīvo akts) nosaka, kuri darbinieki varēs piekļūt vienai vai kādai konkrētai informācijai, lai arī nosauka to, kādai darbības ar sistēmu ir atļautas. Darbiniekam atbilstoši to veicinājam darba pienākumu veikšanai nepieciešamās lomas. Savukārt nodarbinotais ar savu darbību esošo informāciju var rīkoties, nepārkāpjot darba devēja vai normatīvo akta noteiktās robežas un skaidri apzinoties datu apstrādes (T) mērķi.

Государственная инспекция данных Латвии (DVI) 12.03.2024 опубликовала руководство по обработке данных с использованием информационных систем и баз данных, содержащих персональные данные, доступ к которым предоставляется в рамках трудовых правоотношений или государственной службы.

Сотрудники, имеющие доступ к информационным системам, содержащим персональные данные государственной важности или для коммерческой деятельности (например, базы данных клиентов или государственные реестры), должны действовать в рамках нормативных актов или полномочий, установленных работодателем. DVI отметил, что доступ к персональной информации должен предоставляться на основании конкретных должностных обязанностей и задач, связанных с этими обязанностями. Таким образом, личный интерес, любопытство или превышение разрешенного доступа по назначению не являются достаточным основанием для просмотра базы данных.

Кроме того, организации, предоставляющие сотрудникам доступ к таким системам, несут ответственность за применение мер безопасности для ограничения доступа к данным и обеспечение надлежащего обучения сотрудников правилам защиты данных. Таким образом, ответственность за использование данных изначально лежит на организации.

## Право работника на доступ ко всей своей электронной переписке и электронным письмам



**Bundesarbeitsgericht**

Ansicht normal – kontrastreich | Gebärdensprache | Leichte Sprache | Inhalte | Kon

Sie befinden sich hier: [Startseite](#) >> [Pressemitteilungen](#)

**Pressemitteilung Nr. 8/21**

**Erteilung einer „Datenkopie“ nach Art. 15 Abs. 3 DSGVO**

Ein Klageantrag auf Überlassung einer Kopie von E-Mails ist nicht hinreichend bestimmt iSv. § 253 Abs. 2 Nr. 2 ZPO, wenn die E-Mails, von denen eine Kopie zur Verfügung gestellt werden soll, nicht so genau bezeichnet sind, dass im Vollstreckungsverfahren unzweifelhaft ist, auf welche E-Mails sich die Verurteilung bezieht.

Der Kläger war bei der Beklagten vom 1. bis 31. Januar 2019 als Wirtschaftsjurist beschäftigt. Mit seiner Klage hat er ua. Auskunft über seine von der Beklagten verarbeiteten personenbezogenen Daten sowie die Überlassung einer Kopie dieser Daten gemäß Art. 15 Abs. 3 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, im Folgenden DSGVO) verlangt. Nachdem die Beklagte dem Kläger Auskunft erteilt hat, haben die Parteien den Rechtsstreit insoweit für erledigt erklärt.

Die Klage auf Erteilung einer Kopie der personenbezogenen Daten des Klägers hat das Arbeitsgericht abgewiesen. Das Landesarbeitsgericht hat ihr teilweise entsprochen und sie im Übrigen abgewiesen. Es hat angenommen, der Kläger habe zwar einen Anspruch auf Erteilung einer Kopie seiner personenbezogenen Daten, die Gegenstand der Auskunft der Beklagten waren, nicht aber auf die darüber hinaus verlangten Kopien seines E-Mail-Verkehrs sowie der E-Mails, die ihn namentlich erwähnen.

Die gegen die teilweise Abweisung seiner Klage gerichtete Revision des Klägers hatte vor dem Zweiten Senat des Bundesarbeitsgerichts keinen Erfolg. Der Senat konnte offenlassen, ob das Recht auf Überlassung einer Kopie gemäß Art. 15 Abs. 3 DSGVO die Erteilung einer Kopie von E-Mails umfassen kann. Jedenfalls muss ein solcher zugunsten des Klägers unterstellter Anspruch entweder mit einem iSv. § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmten Klagebegehren oder, sollte dies nicht möglich sein, im Wege der Stufenklage nach § 254 ZPO gerichtlich geltend gemacht werden. Daran fehlte es hier. Bei einer Verurteilung der Beklagten, eine Kopie des E-Mail-Verkehrs des Klägers zur Verfügung zu stellen sowie von E-Mails, die ihn namentlich erwähnen, bliebe unklar, Kopien welcher E-Mails die Beklagte zu überlassen hätte. Gegenstand der Verurteilung wäre die Vornahme einer nicht vertretbaren Handlung iSv. § 858 ZPO, für die im Zwangsvollstreckungsrecht nicht vorgesehen ist, dass der Schuldner an Eides statt zu versichern hätte, sie vollständig erbracht zu haben.

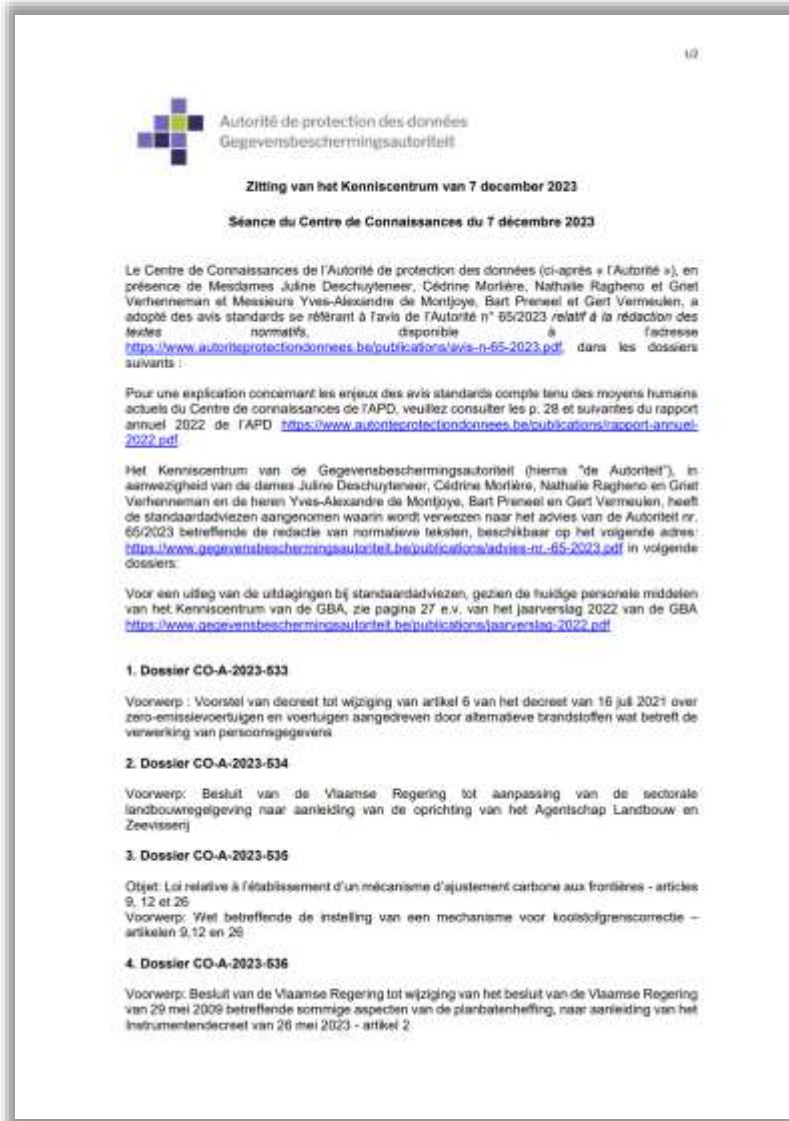
Bundesarbeitsgericht, Urteil vom 27. April 2021 - 2 AZR 342/20 -  
Vorinstanz: Landesarbeitsgericht Niedersachsen, Urteil vom 9. Juni 2020 - 9 Sa 608/19 -

27.04.2021 Федеральный суд по трудовым спорам Германии опубликовал свое решение относительно права работника на доступ ко всей своей электронной переписке и любым электронным письмам, в которых он упоминается по имени. Суд установил, что запрос, который был подан в соответствии со ст.15 GDPR, не был достаточно конкретным в соответствии с применимыми гражданскими процессуальными нормами. В результате суд постановил, что работодатель не был обязан предоставлять копии всей электронной переписки работника, а также любых электронных писем с упоминанием работника по имени.

<https://www.bundesarbeitsgericht.de/entscheidung/2-azr-342-20/>

<https://www.lexology.com/library/detail.aspx?g=2a0f9f6a-3fd8-4032-93e8-6247ebbc49a5>

## Постановление бельгийского АР о незаконности постоянного видеонаблюдения за работниками



Бельгийский орган по защите данных 23.11.2023 постановил, что постоянное наблюдение за работниками магазина с помощью камер видеонаблюдения нарушает принцип минимизации данных ст.5(1)(с) GDPR, поскольку наблюдение не было необходимо для поддержания безопасности.

Работник магазина (субъект данных) подал жалобу на своего работодателя Бельгии, который установил несколько камер видеонаблюдения в магазинах. Субъект данных утверждал, что камеры были установлены таким образом, что сотрудники находились под постоянным наблюдением, что противоречило заявленной цели камер, которая заключалась в обеспечении безопасности в случае кражи или агрессии третьих лиц.

Наблюдение было нарушением [Коллективного трудового договора](#) (CLA) № 68 о защите частной жизни работников в связи с наблюдением за ними на рабочем месте. Наблюдение с помощью камер не может быть непрерывным в отношении производственного процесса и контроля за продуктивностью сотрудников.

<https://www.gegevensbeschermingsautoriteit.be/publications/waarschuwing-en-berisping-nr-154-2023.pdf>

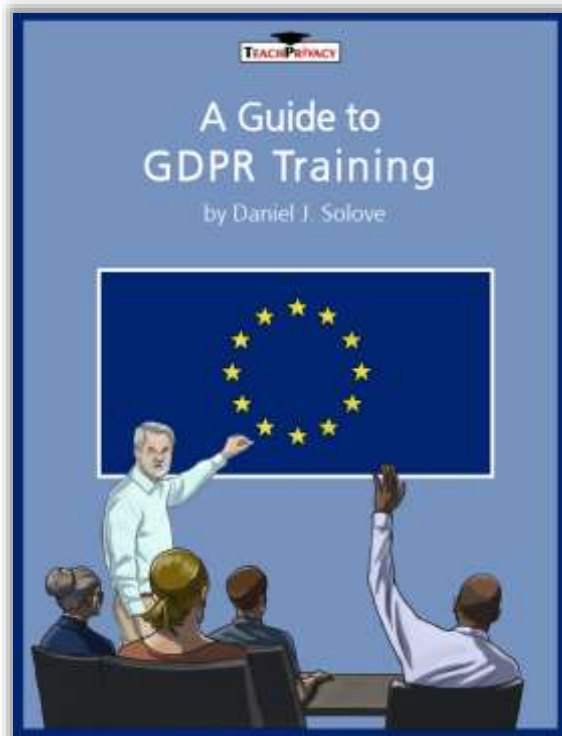
[https://gdprhub.eu/index.php?title=APD/GBA\\_\(Belgium\)\\_-\\_DOS-2023-04114](https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_DOS-2023-04114)

## 382 Соблюдение GDPR при подборе персонала



Ответы от компании SmartRecruiters на часто задаваемые вопросы об обработке персональных данных соискателей при процессе подбора персонала. Рассматриваются общие вопросы обработки персональных данных соискателей, получения их согласия, привлечение третьих лиц к обработке, сбор персональных данных соискателей из открытых источников, документирование процесса подбора персонала с точки зрения требований GDPR.

## Краткое руководство TeachPrivacy по подготовке и проведению тренингов по GDPR



(1) **Motivation:** Why should people care?

(2) **Definition:** What is personal data?

(3) **Responsibilities:** What should people know about the way the organization handles privacy? What should people do in their jobs to protect data?



### *Motivation*

If people don't care, they won't pay attention and won't change their behavior. People need to understand why privacy matters and the concrete implications that violations of privacy can have on individuals, on the organization, and on the workforce members involved in a violation. People pay a lot more attention when they are told why they should be paying attention.

### *Definition*

People need to know what data is covered. People must learn roughly how to identify personal data and sensitive data. A challenge here is that the GDPR has a definition of personal data that is different from how US law defines it. US law defines it in many different ways.

People don't need to know each particular definition — otherwise, their heads would spin. The key goal here is to get people to understand that a lot of data that they might not think is personal data in fact can be personal data. Data that alone is not identified to a particular person can be combined with other data and become identified to that person. So it isn't possible to provide a comprehensive list of all personal data.

My strategy here is to deepen people's understanding and teach them enough so that they ask when they are uncertain and avoid making false assumptions.



### *Responsibilities*

People need to be taught what they should know about how an organization handles its responsibilities for protecting data as well as their role in the process. This can be accomplished by teaching people what protecting privacy entails more conceptually. By this, I mean that training should focus on the Fair Information Practice Principles (FIPPs). The FIPPs are the backbone to most privacy laws, and despite all the differences in privacy laws around the world, the FIPPs have widespread consensus.



#### For whom is this brochure intended?

- › For employees
- › For management
- › For company data protection officers

#### Data protection in the company

- › Company secrets
- › The importance of data protection within the company

#### Legal basis

- › Which laws regulate data protection?
- › When does data protection law permit the processing of personal data?

#### Who is responsible for good data protection?

- › The company management creates the framework conditions
- › The employees carry out the regulations
- › The company data protection officer advises and monitors
- › The data protection supervisory authority advises, monitors and possibly imposes fines

#### Practical tips

- › Is data processing allowed?
- › Is the data subject informed about the data processing?
- › Is the processing of the data secure?
- › Data security rules
- › Store, delete or restrict access to data?
- › Rights of the people affected
- › Data processing by service providers – data processing on behalf
- › Data processing abroad

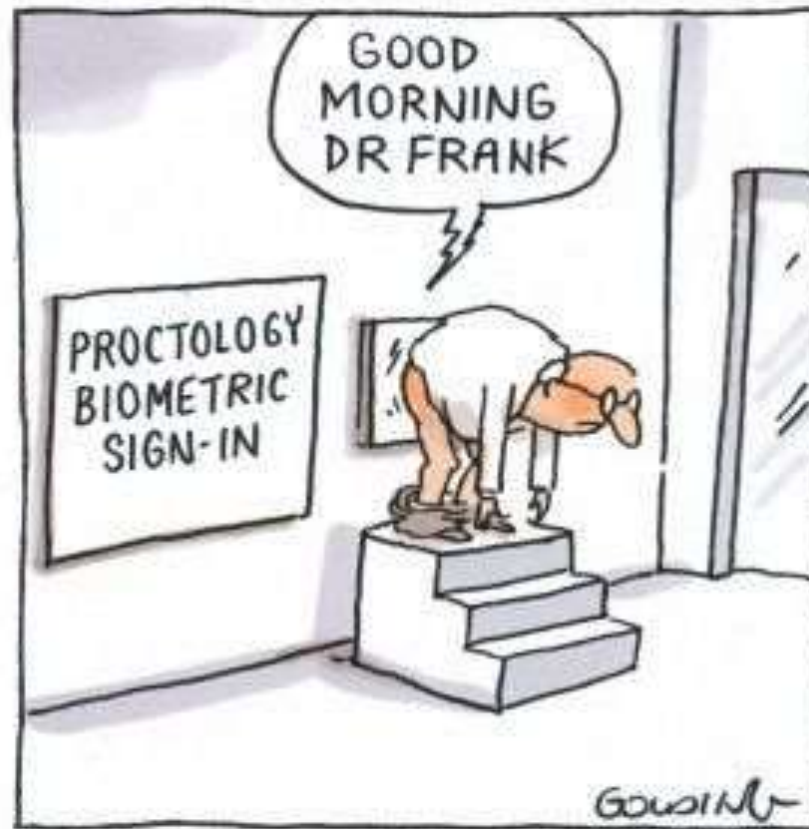
#### What to do in case of data breaches

#### Liability for data protection violations

- › Am I liable to my employer for data protection violations?
- › Labor law consequences
- › Fines
- › Fines and imprisonment



## Биометрические данные и видеонаблюдение



## Использование системы видеонаблюдения и осуществление биометрической идентификации



### "Руководство по распознаванию лиц" (T-PD(2020)03rev4)

*Принято 28.01.2021 Консультативным комитетом Конвенции о защите физических лиц при автоматизированной обработке персональных данных (Конвенция 108)*

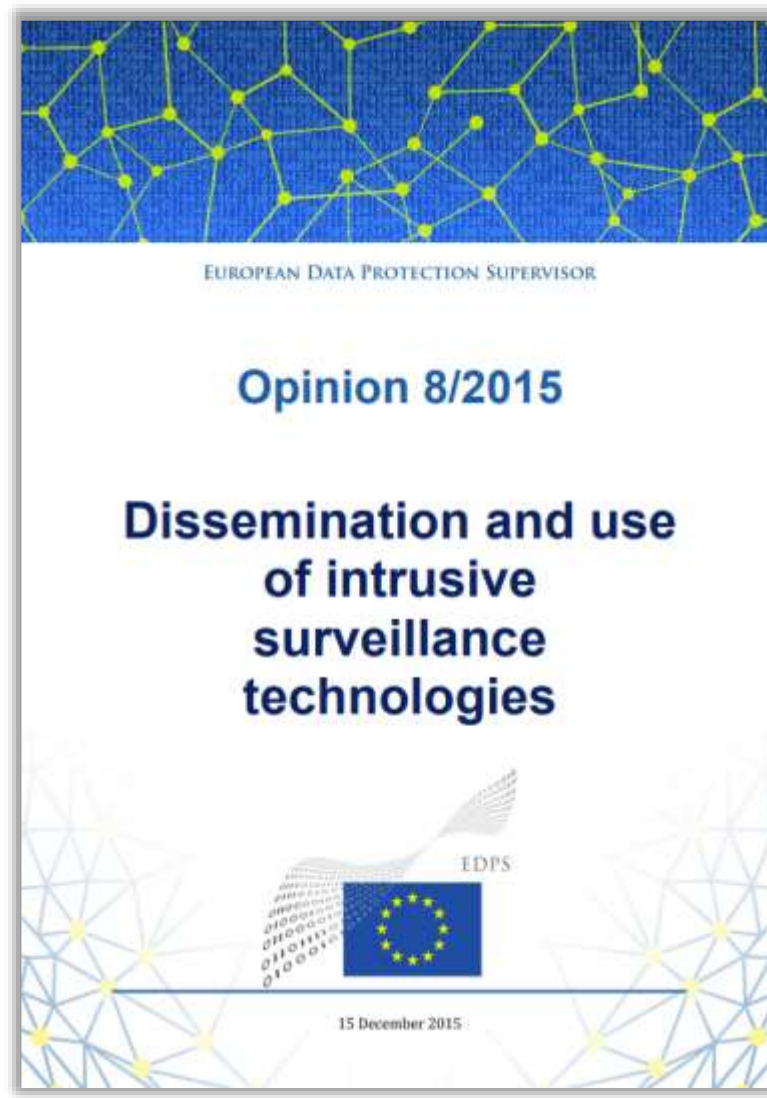
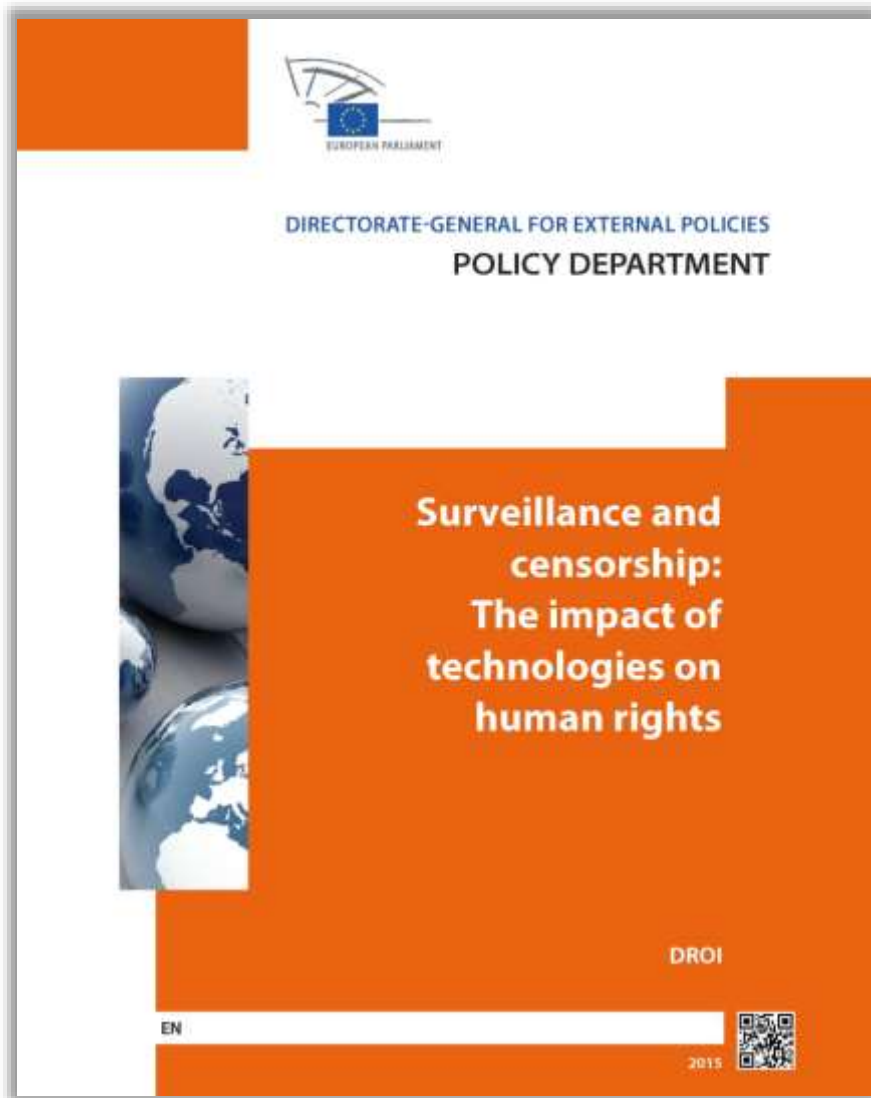
Правомерность использования технологий распознавания лиц должна быть основана на целях биометрической обработки, предусмотренных законом, и на необходимых гарантиях, дополняющих Конвенцию 108+.

Могут быть предусмотрены различные тесты необходимости и соразмерности в зависимости от того, является ли целью идентификация или проверка, с учетом потенциальных рисков для основных прав, при условии, что изображения физических лиц получены законно.

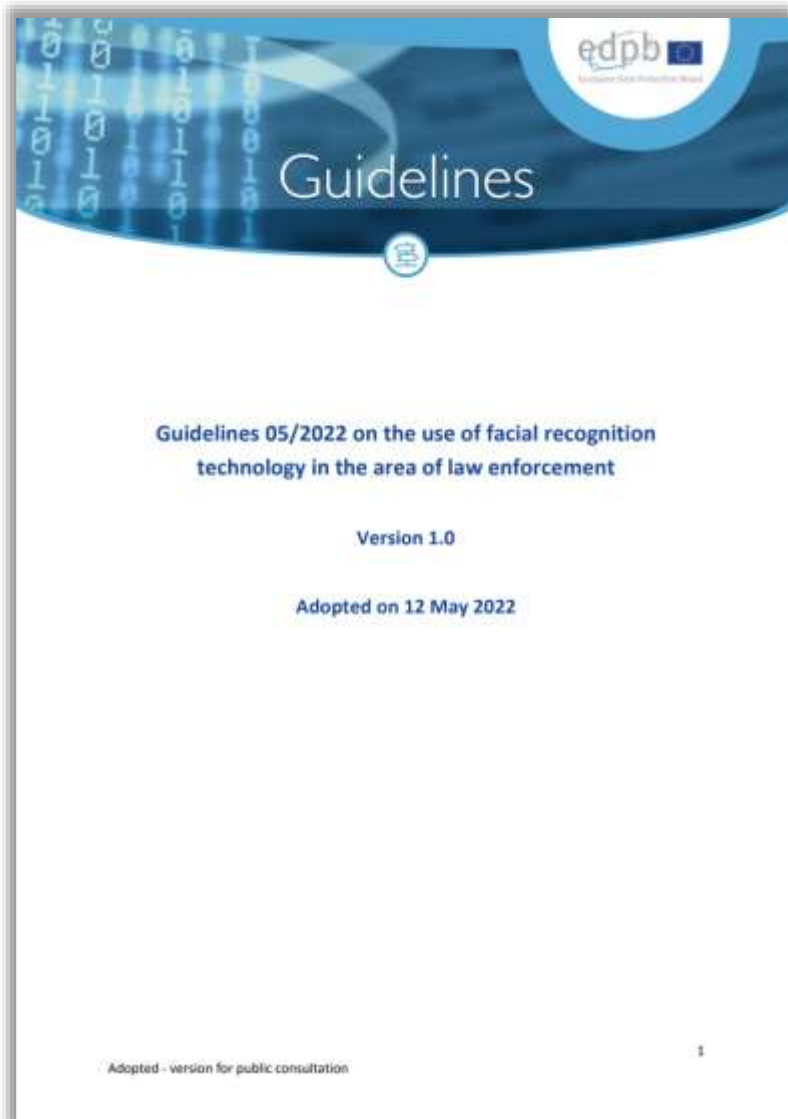
Для целей идентификации требование строгой необходимости и соразмерности должно соблюдаться и на стадии создания базы данных (списка наблюдения), и на стадии развертывания технологий распознавания лиц (онлайн) в неконтролируемой обстановке.

Обеспечение безопасности в контролируемой и неконтролируемой обстановке, в том числе в школах и других общественных зданиях, не должно считаться строго необходимым и соразмерным при наличии менее интрузивных альтернативных механизмов.


## Интрузивные методы слежения: мнение Европейского парламента и European Data Protection Supervisor



## Руководство EDPB по использованию технологии распознавания лиц в правоохранительной деятельности



1	Introduction.....	.....
2	Technology .....	.....
2.1	One biometric technology, two distinct functions.....	.....
2.2	A wide variety of purposes and applications .....	.....
2.3	Reliability, accuracy and risks for data subjects.....	.....
3	Applicable legal framework.....	.....
3.1	General legal framework – The EU Charter of Fundamental Rights (hereinafter “the Charter”) and the European Convention on Human Rights (ECHR).....	.....
3.1.1	Applicability of the Charter .....	.....
3.1.2	Interference with the rights laid down in the Charter .....	.....
3.1.3	Justification for the interference.....	.....
3.2	Specific legal framework – the Law Enforcement Directive .....	.....
3.2.1	Processing of special categories of data for law enforcement purposes.....	.....
3.2.2	Automated individual decision-making, including profiling.....	.....
3.2.3	Categories of the data subjects .....	.....
3.2.4	Rights of the data subject.....	.....
3.2.5	Other legal requirements and safeguards.....	.....
4	CONCLUSION .....	.....
5	Annexes .....	.....
	Annex I - Template for description of scenarios .....	.....
	Annex II- Practical guidance for managing FRT projects in LEAs.....	.....
	Annex III - Practical examples.....	.....



The screenshot shows the official website of the UODO (Urząd Ochrony Danych Osobowych). The header includes the UODO logo, the name of the office, and contact information (Infolinia Urzędu 606-950-000). A search bar is present with the text 'Wpisz frazę której szukasz'. Below the header, there are navigation tabs: 'Prezes i Urząd', 'Prawo', 'Edukacja', and 'Współpraca'. The main content area features a section titled 'Aktualności' (News) with a sub-heading 'Dane biometryczne mogą być wykorzystywane tylko w wyjątkowych sytuacjach'. The article text discusses the risks of biometric data processing, such as identity theft and discrimination, and emphasizes the need for strict data protection measures. It also mentions the 'RODO' (GDPR) and the importance of informed consent. A graphic with the word 'KOMUNIKAT' (Communication) and various icons is also visible.

Urząd Ochrony Danych Osobowych

Wpisz frazę której szukasz

Infolinia Urzędu 606-950-000

Prezes i Urząd    Prawo    Edukacja    Współpraca

📍 + Aktualności

### Dane biometryczne mogą być wykorzystywane tylko w wyjątkowych sytuacjach

Przetwarzanie danych biometrycznych mocno ingeruje w prywatność osób, powoduje liczne zagrożenia, jak np. możliwość ujawnienia danych szczególnych kategorii czy doprowadzenie do dyskryminacji. Dlatego budowa każdego systemu przetwarzania danych biometrycznych powinna być poprzedzona przeprowadzeniem oceny skutków dla ochrony danych, a ostateczna decyzja o jego zastosowaniu uwzględniać podstawowe zasady ochrony danych osobowych, takie jak niezbędność, celowość oraz proporcjonalność.

Rozporządzenie ogólne o ochronie danych osobowych (RODO) nieprzypadkowo co do zasady zabrania przetwarzania danych biometrycznych, poza pewnymi wyjątkami. Dane takie jak odciski palców, wizerunek twarzy, siatkówka czy tętno oka, czy behawioralne lub psychiczne cechy danej osoby, przetwarzane specjalnymi metodami technicznymi, pozwalają nie tylko jednoznacznie nas zidentyfikować i określić, ale są to dane niezmiernie. A więc w ciągu całego naszego życia nie da się ich zmienić, tak jak np. nazwiska, numeru identyfikacyjnego, adresu zamieszkania. Ewentualny wyciek tej szczególnej kategorii danych osobowych - spowodowałby wysokie ryzyko naruszenia praw i wolności osób, których dotyczą. Negatywne konsekwencje takiego zdarzenia mogą mieć miejsce przez całe dalsze życie. Dlatego przetwarzanie danych biometrycznych dopuszczone jest tylko wyjątkowo na podstawie art. 9 ust. 2 RODO gdy m.in. pozwala na to przepis bądź osoba, której dane dotyczą wyraziła na to zgodę.

#### Zgoda również z warunkami

RODO określa, że zgoda musi być jednoznaczna, dobrowolna, świadoma i wyrażona wprost przez osoby, których dane dotyczą i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. A więc podstawowymi przesłankami konstrukcyjnymi zgody są dobrowolność, konkretność, świadomość i jednoznaczność. Ponadto wyrażający zgodę powinien wiedzieć, w jakim celu i komu danej zgody udziela.

Wymóg dobrowolności zgody oznacza zaś, że osoba, której dane dotyczą, ma rzeczywisty i wolny wybór co do udzielenia zgody oraz może jej odmówić lub ją wycofać bez niekorzystnych konsekwencji. A więc brak zgody osoby na przetwarzanie jej danych nie może powodować np. dyskryminacji, pogorszenia jakości świadczonych usług czy niemożności skorzystania z niej.

Польский орган по защите данных (UODO) опубликовал 03.03.2021 года руководство по обработке биометрических данных, в котором отмечается, что использование биометрических данных серьезно нарушает конфиденциальность людей и может привести к существенным рискам для субъектов данных или к дискриминации. По этой причине в руководстве подчеркивается, что обработка биометрических данных может происходить только в исключительных обстоятельствах, как указано в ст.9(2) GDPR, при условии проведения оценки воздействия на защиту данных (DPIA) и с учетом основных принципов защиты данных, таких как необходимость, соразмерность и минимизация данных.

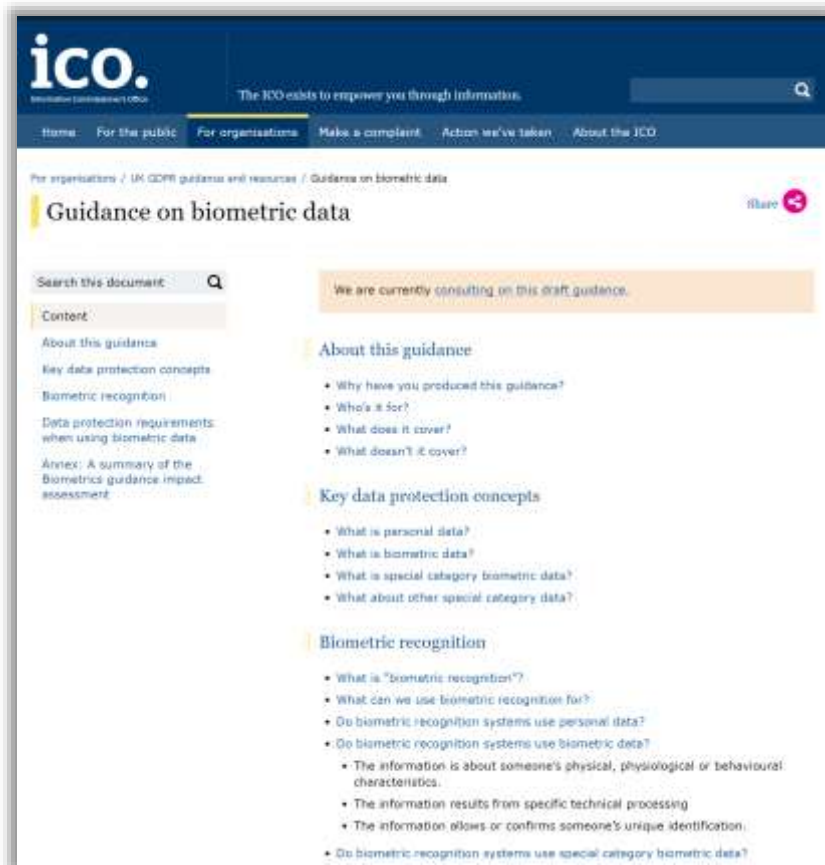
## 390 Разъяснения испанского АЕРД по обработке биометрических данных

Испанский орган по защите данных (АЕРД) опубликовал 26.07.2022 запись в своем блоге под названием "Использование биометрических данных: Оценка с точки зрения защиты данных". В частности, АЕРД отметил, что оценка воздействия обработки биометрических данных на защиту персональных данных (DPIA) должна проводиться в контексте обработки и в связи с ее конечными целями.

АЕРД подчеркнул, что методы обработки биометрических данных основаны на сборе и обработке физических, поведенческих, физиологических или нейронных признаков человека с помощью устройств или датчиков, создающих сигнатуры или модели, которые позволяют идентифицировать, отслеживать или составлять профиль человека. Кроме того, перед использованием любого из методов обработки биометрических данных он должен быть оценен с точки зрения его адекватности, пропорциональности и необходимости, его цели, его влияния на права и свободы физических лиц, а также рисков, которые он влечет за собой, как для человека, так и для общества.

АЕРД предоставил неисчерпывающий список некоторых критериев, которые могут быть полезны при типизации процессов обработки биометрических данных, включая:

- цель операций с биометрическими данными по отношению к цели обработки всех персональных данных;
- правовые основания для обработки биометрических данных;
- объем или степень обработки;
- квалифицированное вмешательство человека в отношении результата биометрической обработки;
- обработка специальных категорий данных;
- прозрачность биометрической обработки и ее результата.

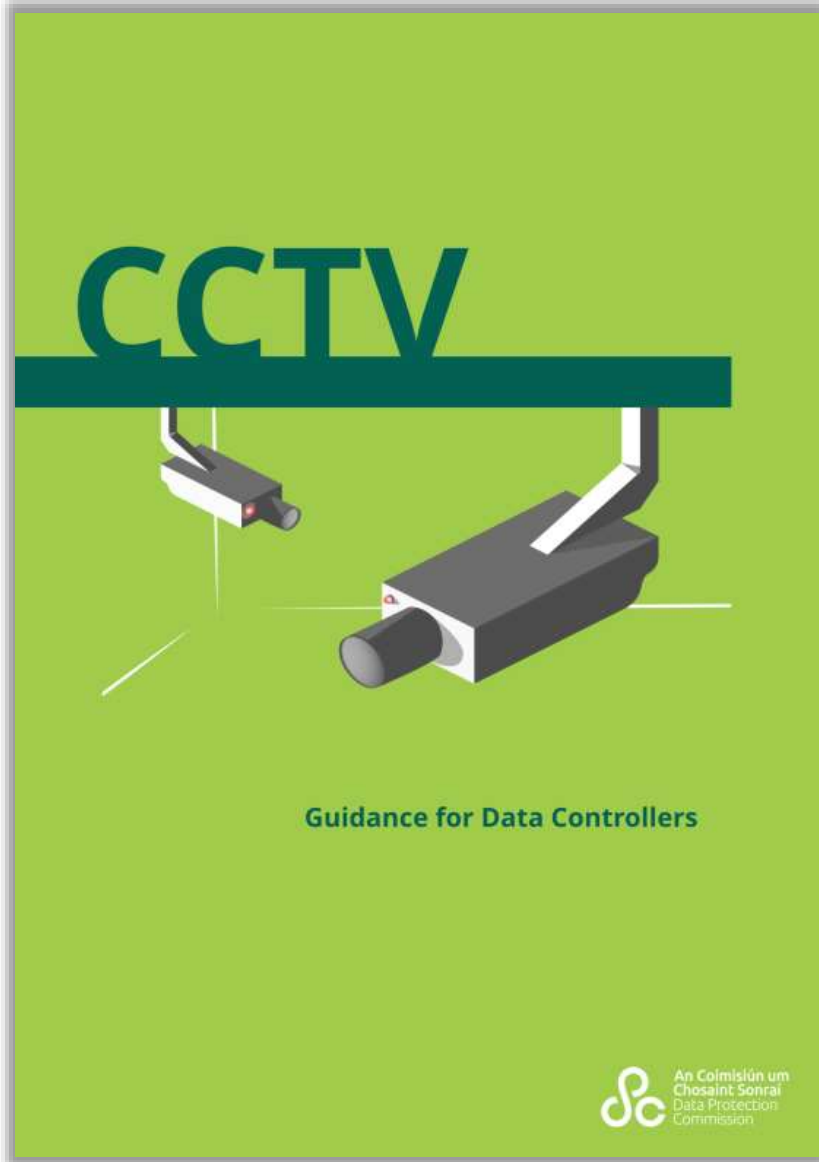


Британское Управление комиссара по информации (ICO) 18.08.2023 начало публичные консультации по проекту своего руководства по биометрическим данным и биометрическим технологиям.

◊ В руководстве подробно описывается, как применяется законодательство о защите данных при использовании биометрических данных в системах биометрического распознавания. Руководство предназначено для организаций, которые используют или рассматривают возможность использования систем биометрического распознавания. В руководстве, в частности, рассматриваются следующие вопросы:

- определение биометрических данных и биометрических данных специальной категории;
- как биометрические данные используются в системах биометрического распознавания;
- законодательные требования к защите данных при использовании биометрических данных, в том числе, когда требуется проведение оценки воздействия на защиту данных (DPIA).

◊ Кроме того, руководство содержит краткое изложение проекта оценки воздействия на защиту биометрических данных. Однако в руководстве не рассматриваются требования к защите данных для правоохранительных органов или служб безопасности.



Introduction .....	
CCTV Checklist.....	
Recommended Data Protection Policy .....	
Purpose of Utilising CCTV.....	
Lawfulness of Processing .....	
Necessity and Proportionality .....	
Necessity and Proportionality Assessment - Examples.....	
Transparency and Accountability .....	
Security of Personal Data.....	
Data Protection By Design and By Default.....	
Data Processors.....	
Retention of Personal Data.....	
CCTV in the Workplace .....	
Case Study .....	
Disclosure of CCTV to Third Parties .....	
Providing Access to CCTV to Data Subjects .....	
Covert Surveillance .....	
Facial Recognition and Biometric Data .....	



## 393 Руководство датского Datatilsynet по использованию компаниями видеонаблюдения



Датский орган по защите данных (Datatilsynet) опубликовал 27.06.2023 новое руководство по видеонаблюдению, которое компании должны принимать во внимание в связи с использованием CCTV. В руководстве указывается:

- когда то или иное действие приравнивается к наблюдению с помощью систем видеонаблюдения;
- в каких случаях компании разрешается вести видеонаблюдение;
- как компании могут выполнить свою обязанность по раскрытию информации лицам, за которыми ведется наблюдение;
- правила хранения и раскрытия записей камер видеонаблюдения;
- права субъектов данных в связи с видеонаблюдением;
- использование обработчиков данных для ведения видеонаблюдения.

## Руководство датского Datatilsynet по использованию видеонаблюдения жилищными товариществами



Датский орган по защите данных (Datatilsynet) 13.12.2023 опубликовал руководство для жилищных товариществ в связи с использованием ими видеонаблюдения. руководстве указывается:

- какие действия приравниваются к видеонаблюдению;
- когда разрешено видеонаблюдение, включая правовые основания;
- как товарищества могут выполнить свою обязанность по раскрытию информации лицам, за которыми ведется наблюдение;
- правила хранения и хранения записей камер видеонаблюдения;
- требования безопасности в отношении видеонаблюдения;
- права субъектов данных в связи с видеонаблюдением, включая доступ и возможность переноса;
- привлечение обработчиков данных.

<https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/dec/nye-vejledninger-om-tv-overvaagning>

<https://www.datatilsynet.dk/Media/638380803505815050/Vejledning%20om%20TV-overv%C3%A5gning%20til%20boligorganisationer.pdf>

## 395 Руководство чешского UOOU по использованию систем видеонаблюдения

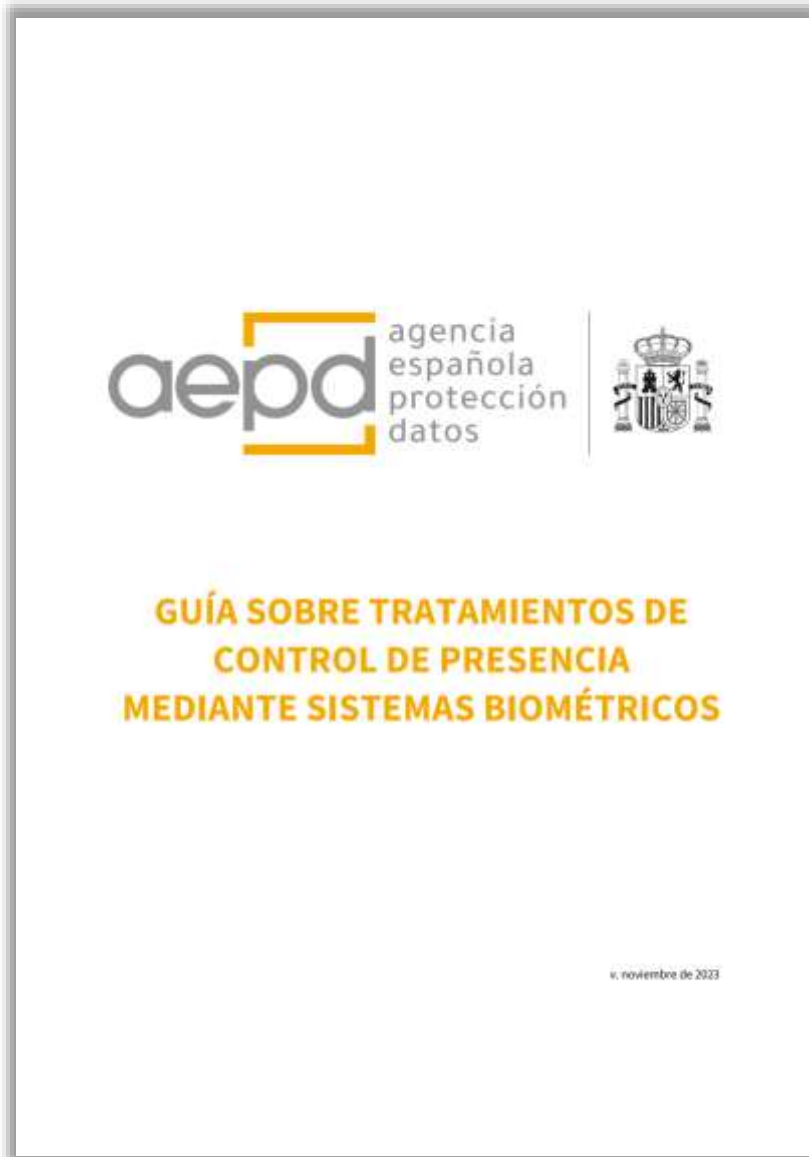
### Metodika

k návrhu a provozování kamerových systémů  
z hlediska zpracování a ochrany osobních údajů

Verze 0.98.3 ze dne 24. dubna 2023

Чешское Управление по защите персональных данных ("UOOU") 28.04.2023 опубликовало руководство проектирования и эксплуатации систем видеонаблюдения в контексте обработки и защиты персональных данных. Цель руководства заключается в обеспечении лучшей методологии для контролеров и обработчиков персональных данных, а также поставщиков систем видеонаблюдения в их обязательствах, связанных с проектированием, установкой и эксплуатацией таких систем. Документ касается систем видеонаблюдения (включая камеры-ловушки) с возможностью записи, а также систем видеонаблюдения, работающих в режиме реального времени.

## Руководство испанского AEPD по использованию биометрических данных для контроля присутствия и доступа



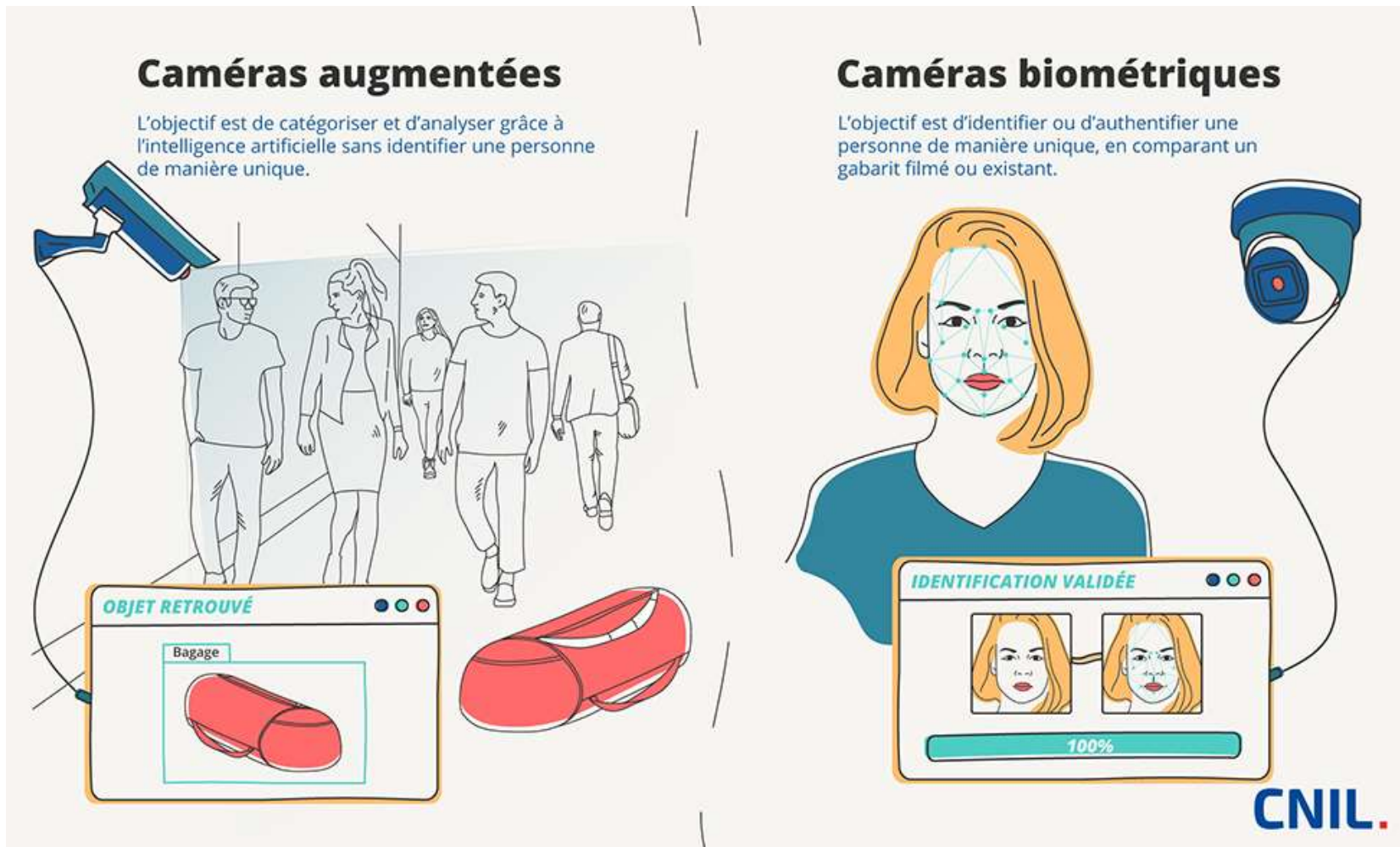
Испанский орган по защите данных (AEPD) 23.11.2023 опубликовал руководство, в котором обработка биометрических данных, как для идентификации, так и для аутентификации, рассматривается как высокорискованная, связанная с особыми категориями данных.

В контексте деятельности, связанной с трудоустройством, такой как регистрация рабочего времени и контроль доступа, руководство подчеркивает необходимость юридического разрешения, конкретно разрешающего использование биометрических данных. Примечательно, что в нем подчеркивается недостаточность одного лишь согласия для подтверждения законности этого процесса, ссылаясь на присущий ему дисбаланс между субъектом данных и организацией, осуществляющей их обработку. Кроме того, руководство распространяет эти критерии на контроль доступа в сценариях, не связанных с трудоустройством.

Более того, руководство также устанавливает ограничения на биометрическую обработку, осуществляемую для контроля присутствия, когда без вмешательства человека принимаются автоматизированные решения, имеющие юридические последствия для человека или существенно влияющие на него подобным образом.

## Разъяснения от CNIL о разнице между видеонаблюдением с использованием биометрии и "дополненным" видеонаблюдением

Французский надзорный орган (CNIL) 19.07.2022 опубликовал разъяснения о разнице между видеонаблюдением с использованием биометрии и "дополненным" видеонаблюдением, которое оснащено ПО с искусственным интеллектом. Например, видеофиксация общественного шоссе для подсчета в реальном времени различных видов участников движения (пешеходы, автомобили, велосипеды) или подсчет и классификация (пол, возраст и т.д.) людей, посещающих торговый центр, чтобы адаптировать содержание рекламы или расположение вывесок или товаров.



**IMU.** Integritetsskydds myndigheten [Kontakta oss](#) [Ordlist](#)

gifier vid kamerabevakning med integritetsvänlig teknik?



### Behandlas personuppgifter vid kamerabevakning med integritetsvänlig teknik?

Publicerad: 4 juli 2023

Digital maskering, pixelering, kameror som inte aktiveras förrän det går ett larm eller reagerar på onormala kroppsrörelser och ljud – idag finns det många sätt att med ny teknik göra kamerabevakning mer integritetsvänlig och göra det svårare att identifiera människor på filmerna.

Шведское управление по защите частной жизни (ИМУ) 04.07.2023 опубликовало разъяснения о последствиях применения в системах видеонаблюдения технологий, обеспечивающих защиту частной жизни, таких как цифровое маскирование и пикселизация. ИМУ пояснило, что первоначальный сбор видеозаписей часто связан с обработкой персональных данных и поэтому регулируется GDPR, а иногда и Законом о видеонаблюдении (CSA).

Также отмечается, что в недавнем надзорном решении, вынесенном в отношении одного из муниципалитетов, ИМУ постановил, что сбор, обработка и передача пикселизированных изображений регулируется CSA. Хотя пикселизация обеспечивает определенный уровень конфиденциальности, она не гарантирует полной анонимности из-за отличительных особенностей, таких как форма тела, характер движений или другие признаки, которые могут быть использованы для идентификации людей. По мнению ИМУ, это особенно актуально в местах, где часто бывают одни и те же люди, например, в школах.

## Руководство латвийского DVI о правомерном проведении фото- и киносъемки с выпускниками

Datu valsts inspekcija

#DVIskaidro "Izaidumu laiks - kas jāņem vērā, fotografējot vai filmējot?"

Publikācija: 10.06.2022

Publikācija: 10.06.2022

Ievērojams izstrādātājam laikam, aizsūtītāji atgūst tēmu par šajās pasākumos uzņemto fotogrāfiju publicēšanu sociālajos tīklos. Lai arī izaiduma laikā noturētie viedokļi var būt šķēršļi, ka nav iespējams atturēties no to aprakstīšanas internetā vārdi, šādas darbības ir jāvērtē, ievērojot citu personu tiesības gan uz privātumu, gan datu aizsardzību.

Skaidrojuma iekšējais divas situācijas - fotogrāfijas publicē izaidumu ziņojumos, viedokļos, absolventu un fotogrāfijas, kuras publicē izaidumu izstrādātājam, mācību sākot, vispārīgās izglītības iestādēs, koleģijas, universitātes.

Jau 2018. gada maģi kļūstām radīsim mītu, ka Vēlākā datu aizsardzības regula (turpmāk-Datu regula) sākoties filmēt vai fotografēt publicē pasākumos un publicēt iegūtos personas datus. Jāatzīmē, ka šādas fotogrāfijas sociālajos tīklos nekad bez atļaujas, kur absolventiem šajā izaidumā ar emocijām un mirsībām ar GDPR.

Privātās un mājasvietas ievērojot jebkuru Datu regulu uz mūsu vietnes?


Situācija, kad veikta publicē savu bērnu fotogrāfijas, draugi savu draugu, un tml., šādi datu apstrāde Datu regulu ievēroti tiek veikta privātām un mājasvietas vajadzībām. [6] Tas nozīmē, ja iegūtos fotoattēlus neapstrādā rādīt šādi par privātu saturu vai šauram draugu lokam - sociālo tīklu personālo notikumu, ierobežot iespēju kādam dalīties ar fotoattēliem, tad minētās darbības ar fotoattēliem neapstrādā Datu regulas tvērumā.

Государственная инспекция данных Латвии ("DVI") опубликовала 10.06.2022 руководство о том, что следует учитывать при проведении фото- и киносъемки с выпускниками.

Если родители публикуют фотографии, например, своих детей или друзей своих детей, то такая обработка данных по смыслу GDPR осуществляется в частных и бытовых целях. Однако в ситуациях, когда изображениями делятся в социальных сетях, не ограничивая, кто может видеть эти изображения, и что позволяет другим делиться фотографиями, публикующее лицо становится контролером, и обработка данных будет подчиняться требованиям GDPR.

Если учебные заведения организуют выпускные мероприятия для выпускников, где планируется фото- или киносъемка, и впоследствии публикуют эти изображения на своем сайте, в социальных сетях, в СМИ или где-либо еще, то такая деятельность подпадает под требования GDPR, поскольку публикация в социальных сетях фотографий, на которых изображены идентифицируемые физические лица, представляет собой обработку персональных данных. Однако DVI определил три возможных правовых основания, которые могут быть применены к такой обработке данных: общественный интерес, законный интерес и согласие.

Кроме того, что учебное заведение должно всегда информировать выпускников об обработке их данных.



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

**Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni**

Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart  
L'Autorità apre istruttorie nei confronti di due Comuni

Faro del Garante sui sistemi di videosorveglianza intelligente.

L'Autorità ha aperto un'istruttoria nei confronti del Comune di Lecco, che ha annunciato l'avvio di un sistema che prevede l'impiego di tecnologie di riconoscimento facciale.

In base alla normativa europea e nazionale, ha ricordato l'Autorità, il trattamento di dati personali realizzato da soggetti pubblici, mediante dispositivi video, è generalmente ammesso se necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Ma i Comuni, ha sottolineato il Garante, possono utilizzare impianti di videosorveglianza, solo a condizione che venga stipulato il cosiddetto "patto per la sicurezza urbana tra Sindaco e Prefettura".

Inoltre, fino all'entrata in vigore di una specifica legge in materia, e comunque fino al 31 dicembre 2023, in Italia non sono consentiti l'installazione e l'uso di sistemi di riconoscimento facciale tramite dati biometrici, a meno che il trattamento non sia effettuato per indagini della magistratura o prevenzione e repressione dei reati. La moratoria nasce dall'esigenza di disciplinare requisiti di ammissibilità, condizioni e garanzie relative al riconoscimento facciale, nel rispetto del principio di proporzionalità.

Il Comune dovrà quindi fornire all'Autorità una descrizione dei sistemi adottati, le finalità e le basi giuridiche dei trattamenti, un elenco delle banche dati consultate dai dispositivi e la valutazione d'impatto sul trattamento dati, che il titolare è sempre tenuto ad effettuare nel caso di "sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

Sempre in materia di videosorveglianza, il Garante ha avviato un'istruttoria anche nei confronti del Comune di Arezzo, dove, secondo notizie di stampa; a partire dal 1° dicembre 2022 è prevista la sperimentazione di "super-occhiali infrarossi" (che rileverebbero le infrazioni dal numero di targa e, collegandosi ad alcune banche dati nazionali, sarebbero in grado di verificare la validità dei documenti del guidatore).

L'Autorità ha messo in guardia dall'uso di dispositivi video che possano comportare – anche indirettamente – un controllo a distanza sulle attività del lavoratore e ha invitato al rispetto delle garanzie previste dalla disciplina privacy e dallo Statuto dei lavoratori.

Anche il Comune di Arezzo dovrà fornire copia dell'informativa che sarà resa agli interessati, sia cittadini a cui si riferiscono i veicoli e sia personale che indosserà i dispositivi, e la valutazione d'impatto sul trattamento dei dati che li riguarda.

Управление по защите данных (Garante per la protezione dei dati personali) 14.11.2022 вынесло официальные постановления двум муниципалитетам - южно-итальянскому городу Лечче и тосканскому городу Ареццо в связи с их экспериментами с биометрическими технологиями.

Управление запретило системы распознавания лиц, использующие биометрические данные, до принятия специального закона, регулирующего их использование.

Однако было добавлено исключение для технологии биометрических данных, которая используется "для борьбы с преступностью" или в рамках судебного расследования.



# RECONNAISSANCE FACIALE

## POUR UN DEBAT À LA HAUTEUR DES ENJEUX

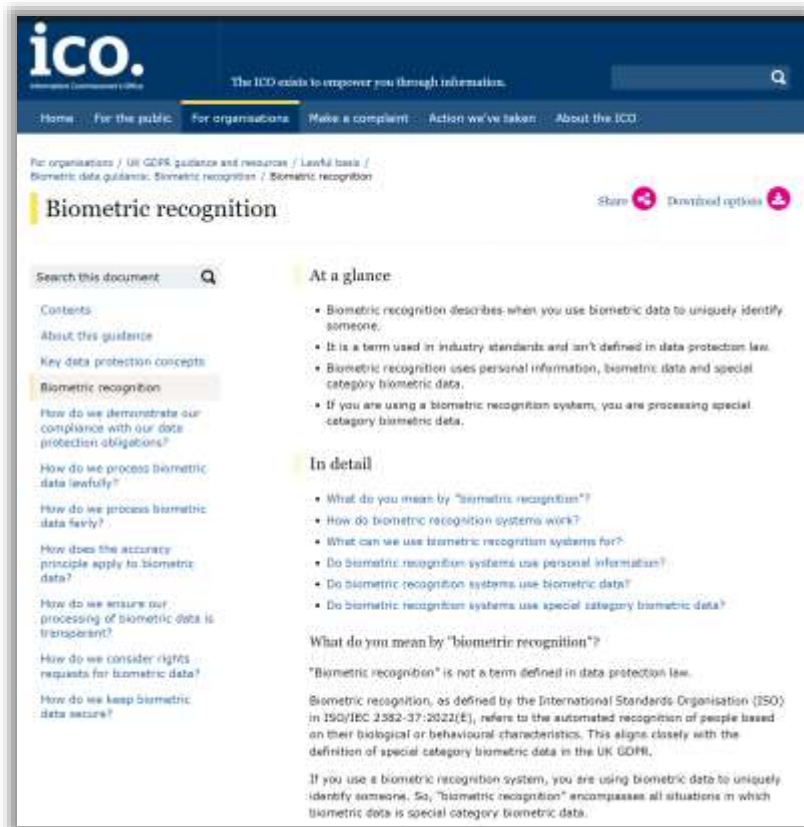
*La reconnaissance faciale est de plus en plus présente dans le débat public au niveau national, européen et mondial et soulève en effet des questions inédites touchant à des choix de société. C'est pourquoi la CNIL avait appelé, en 2018, à un débat démocratique sur ce sujet, ainsi que plus largement sur les nouveaux usages de la vidéo. Elle souhaite aujourd'hui contribuer à ce débat, en présentant les éléments techniques, juridiques et éthiques qui doivent selon elle être pris en compte dans l'approche de cette question complexe.*

Introduction .....	2
I - La reconnaissance faciale : de quoi parle-t-on exactement ? .....	3
1. La reconnaissance faciale est une technologie biométrique de reconnaissance des visages .....	3
2. La reconnaissance faciale n'est pas synonyme de vidéo « intelligente » .....	4
3. Derrière « la » reconnaissance faciale, des cas d'usage pluriels .....	4
II - Les impacts de la reconnaissance faciale : quels sont les risques de cette technologie ? .....	6
1. Des données particulièrement sensibles, faisant l'objet d'une protection particulière .....	6
2. Une technologie sans contact et potentiellement omniprésente .....	7
3. Un potentiel de surveillance inédit, pouvant mettre en cause des choix de société .....	7
4. Des technologies faillibles et coûteuses, appelant un bilan complet et lucide .....	8
III - Expérimenter la reconnaissance faciale ? Dans un cadre précis et avec méthode .....	9
1. Première exigence : tracer des lignes rouges, avant même tout usage expérimental .....	9
2. Deuxième exigence : placer le respect des personnes au cœur de la démarche .....	10
3. Troisième exigence : adopter une démarche sincèrement expérimentale .....	10
IV - Quel rôle pour la CNIL dans la régulation de la reconnaissance faciale ? .....	11

## Commission nationale de l'informatique et des libertés

Французский надзорный орган CNIL опубликовал отчет, проливающий свет на дебаты и дискуссии о применении технологий распознавания лиц. Документ описывает:

- что такое распознавание лиц и для чего оно используется;
- технологические, этические и социальные риски, связанные с этими технологиями;
- какова должна быть роль CNIL при внедрении новых устройств распознавания лиц;
- правила и ограничения в отношении технологий распознавания лиц, которые должны соблюдаться при создании новых устройств.



Британский регулятор в сфере защиты персональных данных ICO (Informational Commissioner's Office) 04.03.2024 опубликовал руководство по биометрическим данным. В руководстве рассказывается о том, как законы о защите данных применяются при использовании биометрических систем распознавания.

Руководство предназначено в первую очередь для организаций, которые используют или рассматривают возможность использования систем биометрического распознавания, а также для поставщиков этих систем, включая продавцов и разработчиков. Кроме того, в руководстве рассматривается определение биометрических данных в соответствии с UK GDPR, уделяется особое внимание их применению в системах биометрического распознавания, разъясняется порядок обработки биометрических данных особой категории и излагаются необходимые требования к защите данных для обеспечения соответствия.

Примечательно, что в руководстве разъясняется, что "биометрическое распознавание" не имеет четкого определения в законодательстве о защите данных. В руководстве поясняется, что определение Международной организации по стандартизации (ISO) в ISO/IEC 2382-37:2022(E) характеризует биометрическое распознавание как автоматизированное распознавание людей на основе их биологических или поведенческих характеристик. В руководстве подчеркивается, что это определение полностью соответствует определению биометрических данных особой категории в UK GDPR.

## EDPB и EDPS призвали запретить применение искусственного интеллекта для распознавания лиц



Два ведомства Евросоюза 21.06.2021 призвали полностью запретить применение искусственного интеллекта для распознавания лиц и других способов идентификации людей в общественных местах. Ранее Еврокомиссия предложила жестко ограничить, но не запрещать полностью использование ИИ в этой области.

"Если мы хотим сохранить наши свободы и создать ориентированное на человека законодательство об ИИ, то начать следует с общего запрета на системы распознавания лиц в общественных местах", - сказано в совместном заявлении глав Европейского совета по защите данных (The European Data Protection Board, EDPB) и Европейского надзорного органа по защите данных (European Data Protection Supervisor, EDPS) Андреа Елинек и Войцеха Вевэровского.

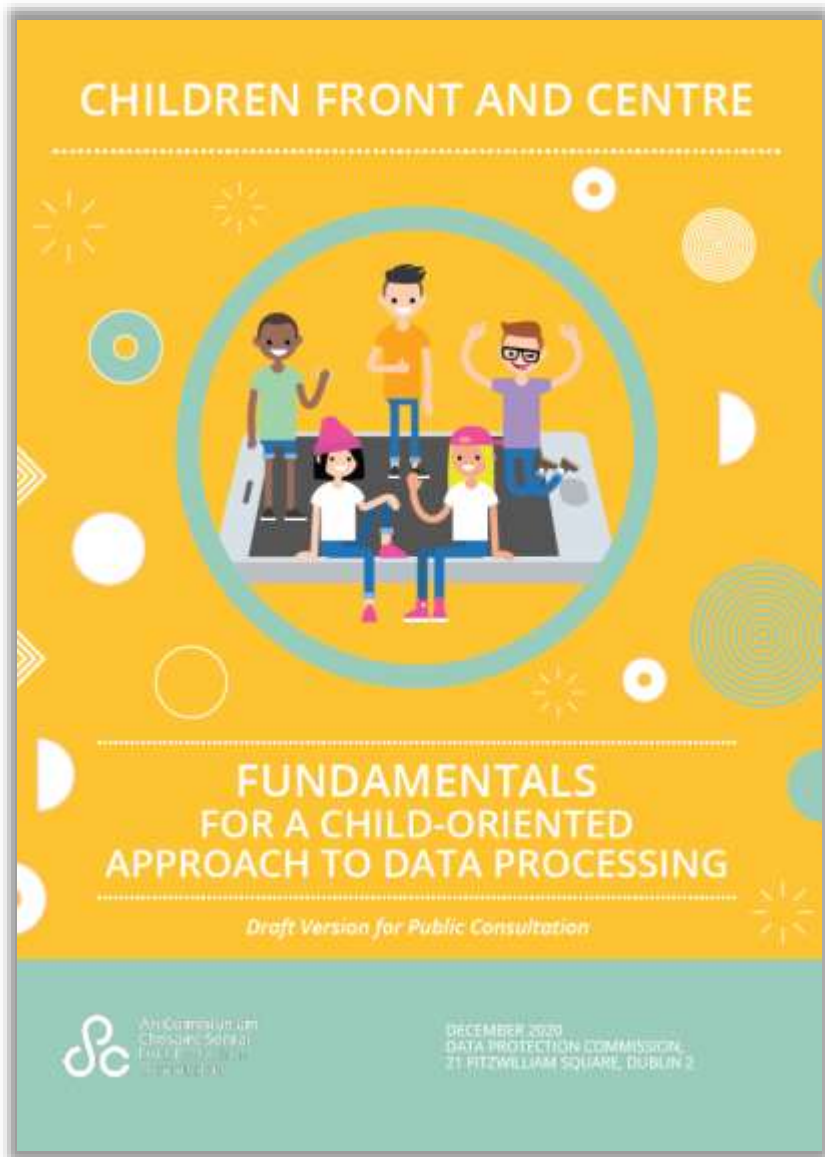
Они призывают запретить в общественных местах программы идентификации людей и по лицу, и по походке, по голосу, отпечаткам пальцев, ДНК и прочим биометрическим и поведенческим признакам.

Кроме того, главы EDPB и EDPS считают, что ЕС должен запретить и системы ИИ, которые классифицируют людей по этническому происхождению, полу, политическим взглядам или сексуальной ориентации. Применение систем, распознающих эмоции человека, они предлагают разрешить только в очень ограниченном наборе случаев - например, в медицине.

## Обработках данных несовершеннолетних лиц



## Основы ориентированного на детей подхода к обработке данных от ирландского DPC



Ирландская Комиссия по защите данных (Data Protection Commission) опубликовала для публичного обсуждения документ под названием «Основы ориентированного на детей подхода к обработке данных» (Fundamentals for a Child-Oriented Approach to Data Processing). Документ призван дать надлежащую интерпретацию принципов защиты данных для детей и определить рекомендуемые меры повышения уровня защиты данных детей при потреблении ими услуг как в онлайн-, так и в офлайн-мире.

## Руководство норвежского Datatilsynet по получению согласия на обработку данных несовершеннолетних



### Samtykke fra mindreårige

Barn kan være mindre bevisste på risikoer og konsekvenser forbundet med deling av personopplysninger. Dette gjør at reglene for behandling av barns personopplysninger er litt annerledes enn for voksne.

Hovedregelen er at barn kan samtykke alene til deling og behandling av egne personopplysninger først når de fyller 18 år (jf. vergemålsloven § 9 om rettslig handleevne). Før dette må foreldrene eller den med foreldreansvar samtykke på barnets vegne. Merk likevel at barn har rett til økt selv- og medbestemmelse med alderen, og at foreldrene derfor bør høre med barna selv før de samtykker på deres vegne (barneloven § 33).

Barn under 18 år kan i noen situasjoner gi samtykke selv dersom de er i stand til å gi et informert og frivillig samtykke (jf. barneloven § 33 og de alminnelige kravene til gyldig samtykke). Dette må vurderes blant annet etter barnets modenhet, og om informasjonen som gis er tilpasset barnets alder og evne til å forstå hva det gir samtykke til. Husk at et samtykke skal gjelde spesifikt for den aktuelle behandlingen. En tommelfingerregel kan være at jo større personvernkonsekvenser behandlingen av opplysninger vil kunne ha, desto høyere terskel bør det være for at barnet kan samtykke selv, uten foreldre.

[Les mer om hva et gyldig samtykke er](#)

I tillegg gjelder det egne regler for når en mindreårig kan gi samtykke på flere områder. Vi vil gå gjennom reglene for noen av de mest praktiske situasjonene under. Merk likevel at de generelle kravene til gyldig samtykke må være oppfylt.

Норвежский орган по защите данных («Datatilsynet») опубликовал в апреле 2022г. обновленную версию своего руководства по получению согласия на обработку данных несовершеннолетних. Согласно руководству, дети могут давать согласие на обработку своих данных только по достижении ими 18-летнего возраста, а до достижения этого возраста родители или лицо, несущее родительскую ответственность, должно дать согласие от имени ребенка. Родители должны посоветоваться с детьми перед принятием такого решения.

Кроме того, дети в возрасте до 18 лет могут в некоторых ситуациях давать согласие, но его правомерность должна оцениваться исходя из зрелости ребенка, а также адаптированности и понятности текста согласия для определенной возрастной категории. Общее же правило заключается в том, что чем больше потенциальный риск для информационной приватности ребенка, тем выше должен быть порог предоставления возможности ребенку самостоятельно дать согласие.

## Инструменты, шаблоны и рекомендации ICO по самооценке соблюдения прав детей при использовании онлайн-сервисов

27.04.2022 Управление Комиссара УК по информации («ICO») опубликовало самооценку, включающую инструменты, шаблоны и рекомендации, которые призваны помочь онлайн-сервисам соблюдать прав детей. Самооценка состоит из четырех шагов:

1. Понимание прав ребенка;
2. Определение воздействия на права;
3. Оценка воздействие на права;
4. Определение приоритетных действий.



## 408 Исландские руководства по защите детей в цифровой среде



29.04.2022 исландский надзорный орган по защите персональных данных (Persónuvernd), омбудсмен по делам детей (umboðsmaður barna) и Комиссия по СМИ (Fjölmiðlanefnd) опубликовали следующие руководства:

1. Руководство для лица, ответственного за защиту детей в цифровой среде
2. Руководство для работников школ, учреждений детского досуга и спорта
3. Руководство для родителей - Интернет, социальные сети и конфиденциальность.



## Норвежский Datatilsynet опубликовал заявление о видеонаблюдении за молодыми сотрудниками



Datatilsynet

### Kameratilsyn hos virksomheter med unge arbeidstakere

Datatilsynet vil gjennomføre flere kameratilsyn innenfor arbeidsliv fremover. Hovedfokuset er arbeidsplasser med unge arbeidstakere.

Unge arbeidstakere er ekstra sårbare i møtet med arbeidslivet. Samtidig ser Datatilsynet at unge arbeidstakerne ofte blir utsatt for ulovlig kameraovervåking.

– Vi i Datatilsynet ser alvorlig på dette. Planen er derfor å gå på flere uanmeldte stedlige tilsyn. Det betyr at vi kommer til virksomheten uten å varsle om dette på forhånd, sier juridisk seniørrådgiver Marte Lindblad Skaslien.

#### Har mottatt flere tips

Vi har mottatt flere tips om virksomheter med kameraovervåking. Mange sier der at arbeidsgiveren bruker kamera til å se hva de ansatte gjør, eller hvordan de gjør jobben sin.

– Vi ser blant annet en økende bruk av fjerntilgang. Ved bruk av fjerntilgang kan arbeidsgiveren følge med på hva den ansatte gjør, uten å selv være tilstede, sier Skaslien. Hun understreker at dette ofte vil være ulovlig. – Vi får også en del tips om at arbeidsgiveren overvåker pauserom, kontor og andre oppholdsrom. Dette er sjelden tillatt.

13.09.2023 норвежский орган по защите данных (Datatilsynet) опубликовал заявление по поводу видеонаблюдения на рабочем месте, уделив особое внимание молодым сотрудникам. Datatilsynet подчеркнул, что молодые сотрудники более уязвимы на рабочем месте и часто становятся объектами незаконного видеонаблюдения.

Кроме того, в Datatilsynet поступили сообщения о случаях наблюдения за сотрудниками в комнатах отдыха, офисах и других жилых помещениях, что редко допускается. Для борьбы с этим с лета 2023 года Datatilsynet начал проводить проверки на предприятиях.

# Рекомендации WEF по разработке и использованию ИИ в отношении несовершеннолетних лиц

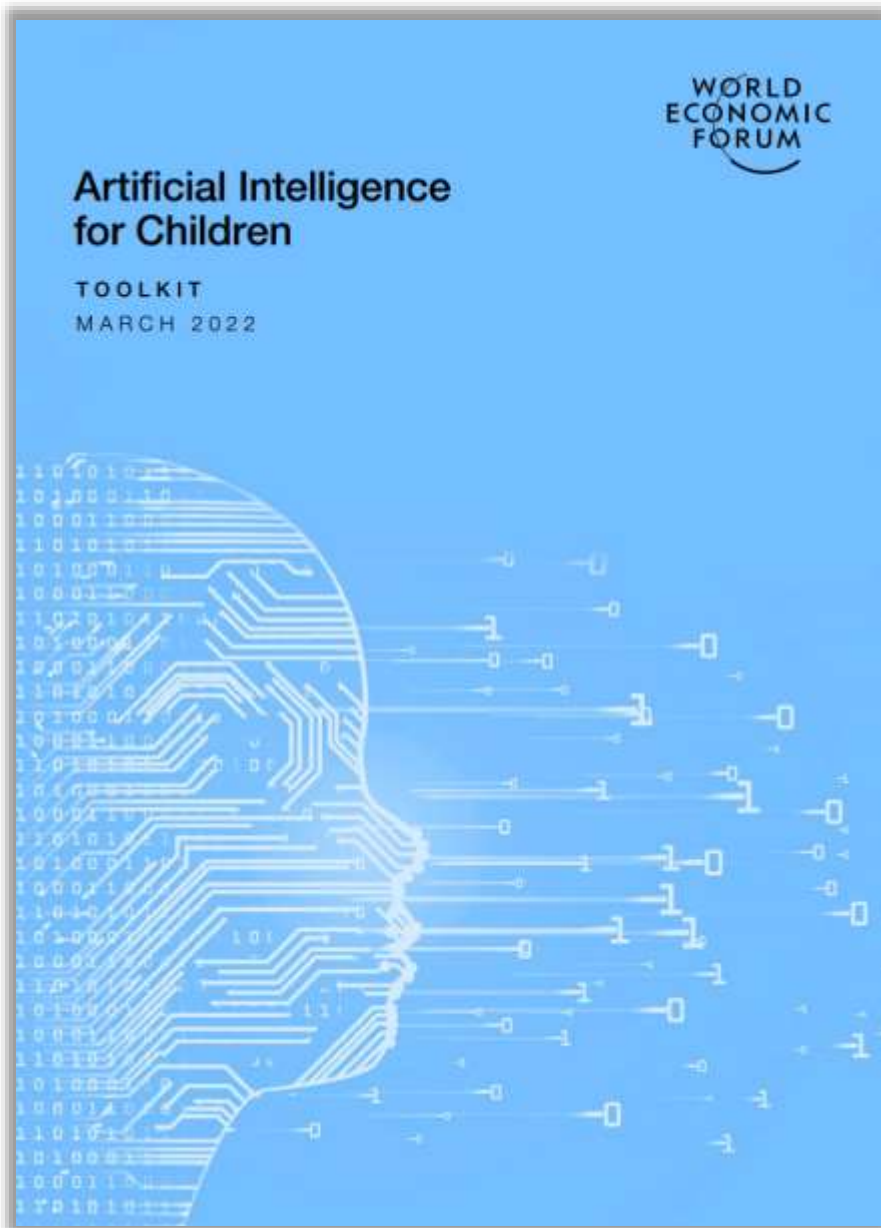
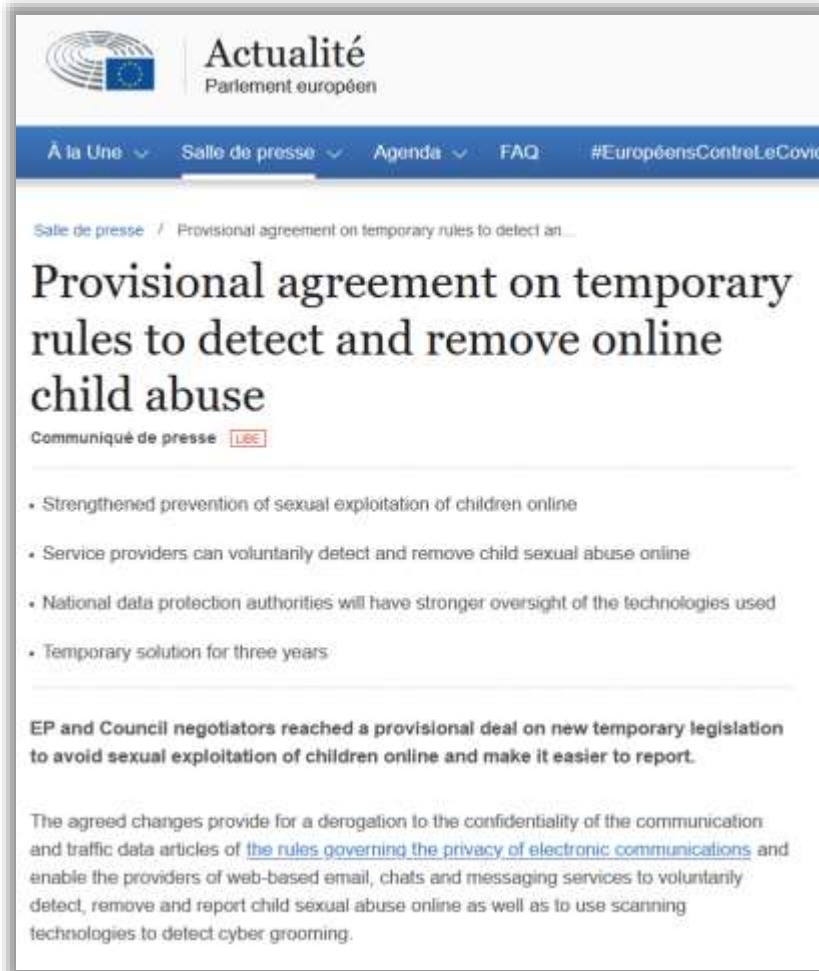


FIGURE 4 Checklist – Putting children and youth FIRST

	Goals	Greatest potential for harm	Mitigate risks
<b>Fair</b>	<ul style="list-style-type: none"> <li>Fairness for the user and their dignity are paramount</li> <li>Bias in training, expression and feedback in the AI is assumed and actively addressed</li> <li>Effort is spent understanding liability</li> <li>Treatise analysis includes how the AI could be weaponized for harm</li> </ul>	<ul style="list-style-type: none"> <li>Breaches of trust and consent</li> <li>Emotional and developmental harm</li> <li>Bias, unequal access and impact</li> </ul>	<ul style="list-style-type: none"> <li>Employ proactive strategies for responsible governance</li> <li>Use ongoing ethical thinking and imagination</li> <li>Employ ethical governance for fairness</li> <li>Test and train with data to understand the behaviour of the model and its areas of bias</li> </ul>
<b>Inclusive</b>	<ul style="list-style-type: none"> <li>Accessibility is built-in; it is not an afterthought</li> <li>"Inclusive" accounts for and celebrates neurodiversity</li> <li>Technology development cycle and testing includes feedback from children and youth</li> </ul>	<ul style="list-style-type: none"> <li>Exclusion by design</li> <li>Bias in, bias out, bias internalised</li> </ul>	<ul style="list-style-type: none"> <li>Build research plans, advisory councils and participant pools that represent high variability in the target audience</li> <li>Actively seek user experience features that create experiences of exclusion</li> <li>Test and train with data to understand the behaviour of the model and its areas of bias</li> </ul>
<b>Responsible</b>	<ul style="list-style-type: none"> <li>The technology is age-appropriate and has a cognitive-development-stage-appropriate design</li> <li>The technology reflects the latest learning science</li> <li>The technology is created with children and youth at the centre of the design and development process</li> </ul>	<ul style="list-style-type: none"> <li>Technology gone rogue</li> <li>Unpredictable, inflexible AI models</li> <li>Built for small, silly adults</li> </ul>	<ul style="list-style-type: none"> <li>Build advisory councils and research participant pools that represent high variability in the target audience</li> <li>Actively seek user experience features that create negative experiences</li> <li>Overcommunicate privacy and security implications</li> <li>Build conviction around the behaviour of the AI and how it might adjust to a user's development stage</li> </ul>
<b>Safe</b>	<ul style="list-style-type: none"> <li>The technology does no harm to customers and cannot be used to harm others</li> <li>Cybersecurity, including the privacy and security of customer data, is a high priority</li> <li>The potential for over-use is acknowledged and addition mitigation is actively built in</li> </ul>	<ul style="list-style-type: none"> <li>Unintended malicious, oblique or naive usage</li> <li>An unsafe community</li> <li>A cautious observer</li> <li>Demographics allowed to define the user</li> <li>Data privacy and security breaches</li> </ul>	<ul style="list-style-type: none"> <li>Conduct user research to inform scenario planning for malicious use cases and mitigation strategies</li> <li>Build a multivariate measurement strategy</li> <li>Build a transparent, explainable and user data-driven relationship model between the child, guardian and technology to identify and mitigate harm</li> <li>Have the product team develop subject-matter expertise in technology concerns related to children and youth</li> <li>Build a security plan that takes children's and youth's cognitive, emotional and physical safety into account</li> </ul>
<b>Transparent</b>	<ul style="list-style-type: none"> <li>Everyone on the team can explain how the AI works and what the AI is being used for to a novice or lay audience</li> <li>Anyone who wants to understand the AI is easily able to do so</li> </ul>	<ul style="list-style-type: none"> <li>Lack of obtusation of informed consent</li> <li>Skirted or ignored governmental rules and regulations</li> <li>The burden of security and privacy is left to the user</li> <li>Excluded guardians</li> </ul>	<ul style="list-style-type: none"> <li>Confirm the terms of use are clear, easy to read and accessible to a non-technical, naive user</li> <li>Clearly disclose the use of high-risk technologies, such as face recognition and emotion recognition, and how this data is managed</li> <li>Explicitly mention the geographic regions whose data protection and privacy laws are honoured by the technology</li> <li>Use more secure options as default and allow guardians to opt-in to advanced features after reading their specific terms of use</li> <li>Clearly specify the age groups for which the application is built</li> <li>Provide guidelines for the environment in which the technology is meant to be used</li> <li>Create alert mechanisms for guardians to intervene in case a risk is identified during usage</li> </ul>

Source: World Economic Forum

## 411 Временные изъятия из Директивы 2002/58/ЕС



The screenshot shows a press release from the European Parliament. At the top left is the logo of the European Parliament with the word 'Actualité' and 'Parlement européen'. Below it is a navigation bar with 'A la Une', 'Salle de presse', 'Agenda', 'FAQ', and '#EuropéensContreLeCovid'. The main title of the press release is 'Provisional agreement on temporary rules to detect and remove online child abuse'. Below the title, it says 'Communiqué de presse' and 'LIBE'. There are four bullet points: 'Strengthened prevention of sexual exploitation of children online', 'Service providers can voluntarily detect and remove child sexual abuse online', 'National data protection authorities will have stronger oversight of the technologies used', and 'Temporary solution for three years'. At the bottom, there is a summary: 'EP and Council negotiators reached a provisional deal on new temporary legislation to avoid sexual exploitation of children online and make it easier to report.' and a paragraph: 'The agreed changes provide for a derogation to the confidentiality of the communication and traffic data articles of the rules governing the privacy of electronic communications and enable the providers of web-based email, chats and messaging services to voluntarily detect, remove and report child sexual abuse online as well as to use scanning technologies to detect cyber grooming.'

Депутаты Европарламента 07.07.2021 одобрили временное постановление, которое позволит цифровым компаниям сканировать переписки для выявления сексуального насилия над детьми на своих платформах и сообщать о них в течение следующих трёх лет. Таким образом компании смогут с помощью программ изучать материалы пользователей для борьбы с недоброжелателями, манипулирующими детьми. Новые правила не распространяются на сканирование аудиосвязи.

Это законодательное изменение было необходимо для того, чтобы позволить поставщикам веб-услуг продолжать применять добровольные меры по борьбе и предотвращению распространения контента сексуального насилия над детьми в Интернете. Прошедшие сканирование данные будут храниться в общей базе не более трёх месяцев и будут немедленно удалены, в случае если в них не было обнаружено противоречивого контента.

Европейские законодатели предупредили, что правила являются «несовершенными с юридической точки зрения». Многие обеспокоены тем, что разрешение компаниям сканировать сообщения открывает им возможность отслеживать другую конфиденциальную информацию. Это мнение было поддержано европейскими регуляторами защиты данных, которые также предупредили, что новое правило нарушает принципы ЕС о конфиденциальности, в частности, GDPR.

## Проект регламента о предотвращении и борьбе с сексуальным насилием над детьми



Еврокомиссия 11.05.2022 представила законодательную инициативу о контроле над чатами, обязующий поставщиков связи проверять содержимое всех частных переписок пользователей на предмет выявления детской порнографии.

Документ предусматривает использование автоматизированной программы, которая будет осуществлять сканирование переписок европейцев и передавать данные на потенциальных нарушителей местным спецслужбам и полиции.

В июле 2021г. Европарламент уже одобрил временное (на 3 года) постановление, получившее названия ePrivacy derogation или Chatcontrol, которое обязало провайдеров цифровых коммуникационных сервисов (email, мессенджеры) сканировать переписки пользователей сервисов для выявления сексуального насилия над детьми на своих платформах и сообщать о них правоохранительным органам.

## Суд в Нидерландах обязал бабушку удалить фотографии её внуков из Facebook



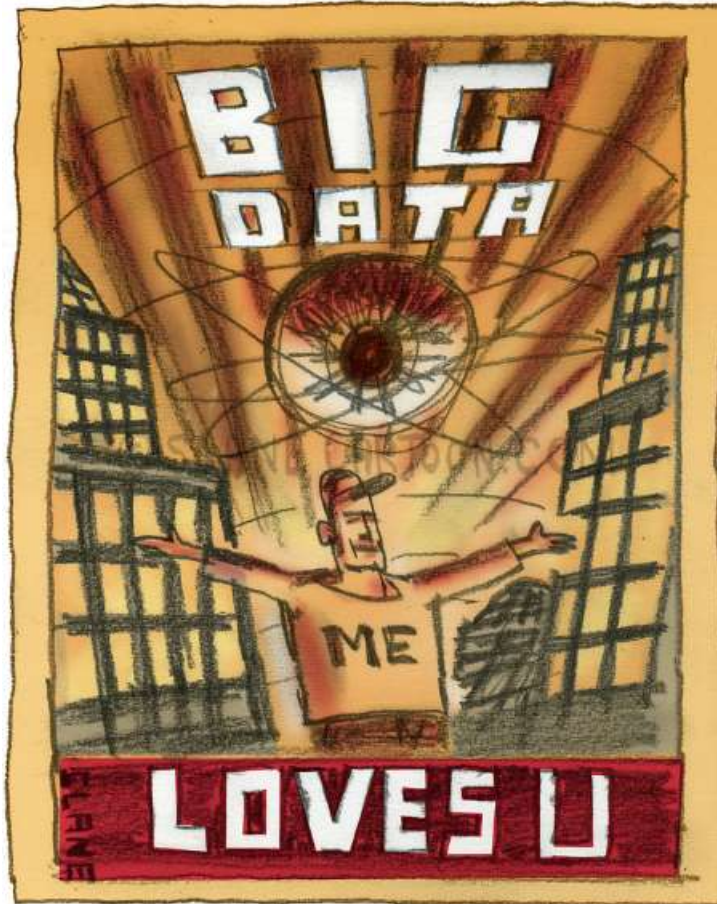
The image shows a screenshot of a BBC News article. At the top, the BBC logo is visible on the left, and navigation links for 'Sign in', 'News', 'Sport', 'Reel', 'Worklife', 'Travel', and 'Future' are on the right. Below this is a red banner with the word 'NEWS' in white. Underneath the banner, there are more navigation links: 'Home', 'Video', 'World', 'UK', 'Business', 'Tech', 'Science', 'Stories', and 'Entertainment & Art'. The article is categorized under 'Technology'. The main headline reads 'Grandmother ordered to delete Facebook photos under GDPR'. Below the headline, it says '© 21 May 2020' and there are social media sharing icons for Facebook, WhatsApp, Twitter, Email, and a general 'Share' button. The main image shows a close-up of an elderly woman's hands holding a smartphone. A 'GETTY IMAGES' watermark is visible in the bottom right corner of the image. Below the image, there is a short summary: 'A woman must delete photographs of her grandchildren that she posted on Facebook and Pinterest without their parents' permission, a court in the Netherlands has ruled.'

Это произошло после ссоры между женщиной и её дочерью. Мать троих детей несколько раз требовала от бабушки удалить фотографии из социальных сетей, в том числе через полицию, однако та отказалась. После этого она обратилась в суд, который постановил, что этот вопрос следует рассматривать в рамках GDPR. Закон не распространяется на «личную» и «бытовую» обработку изображений, однако размещение фотографий в соцсетях сделало их доступным широкой аудитории, говорится в постановлении суда.

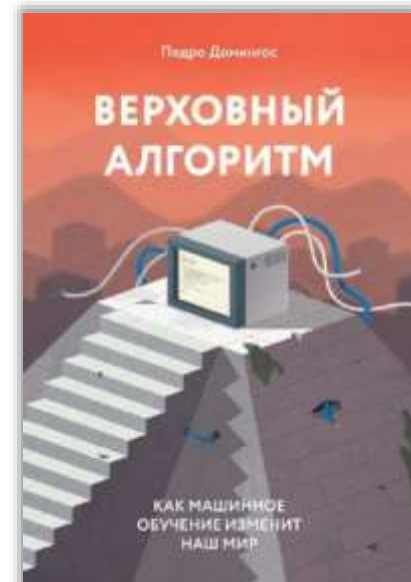
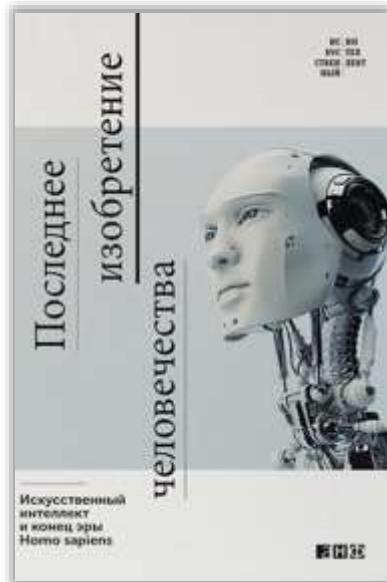
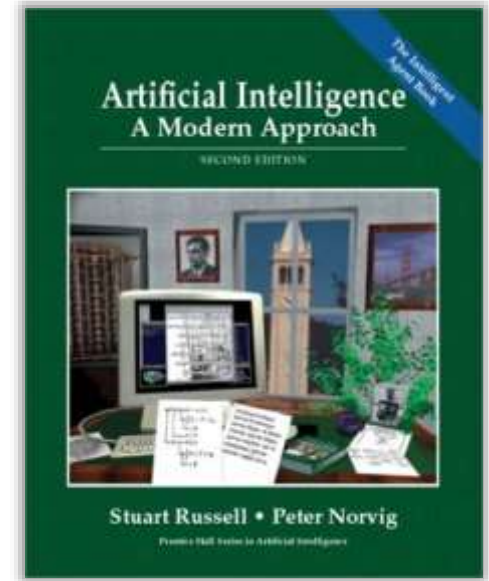
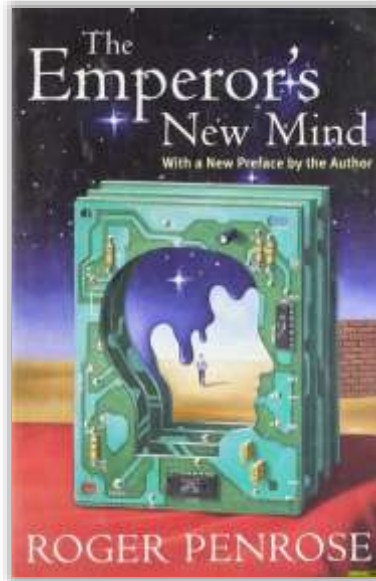
Женщина будет должна либо удалить фотографии, либо заплатить штраф в €50 за каждый день просрочки исполнения требования суда вплоть до максимальной суммы в €1,000. Кроме того, она будет оштрафована ещё на €50 в день за каждую дополнительную опубликованную фотографию.

Решение нидерландского суда отражает позицию, которую Европейский Суд занимал в течение многих лет. Таким образом, вне зависимости от юридических нюансов, было бы разумно, чтобы участники социальных сетей спрашивали себя, согласны люди (или их законные представители/опекуны), запечатленные на фотографиях, на публикацию этих фото в Facebook или Twitter.

# Большие данные, искусственный интеллект, машинное обучение и блокчейн



415 7 книг об искусственном интеллекте



“...the analysis of data to model some aspect of the world. Inferences from these models are then used to predict and anticipate possible future events.”

**UK Government Office for Science. Artificial intelligence: opportunities and implications for the future of decision making. 9 November 2016.**

“...giving computers behaviours which would be thought intelligent in human beings.”

**The Society for the Study of Artificial Intelligence and Simulation of Behaviour. What is Artificial Intelligence. AISB Website. <http://www.aisb.org.uk/public-engagement/what-isai>**

“A set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being. Current developments aim, for instance, to be able to entrust a machine with complex tasks previously delegated to a human.”

**The following definition of AI is currently available on the Council of Europe’s website <https://www.coe.int/en/web/human-rights-rule-of-law/artificial-intelligence/glossary>**

“Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.

AI-based systems can be purely software-based, acting in the virtual world (e.g. **voice assistants, image analysis software, search engines, speech and face recognition systems**) or AI can be embedded in hardware devices (e.g. **advanced robots, autonomous cars, drones or Internet of Things applications**).”

**Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final.**





**Rec.(15)** In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and **should not depend on the techniques used**. The protection of natural persons should apply to the processing of personal data by **automated means**, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system...

**Rec.(71)** The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based **solely on automated processing** and which produces **legal effects** concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention...

## Article 22. Automated individual decision-making, including profiling

1. The data subject shall have **the right not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, **the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests**, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.



**The impact of the General Data Protection Regulation (GDPR) on artificial intelligence**

---

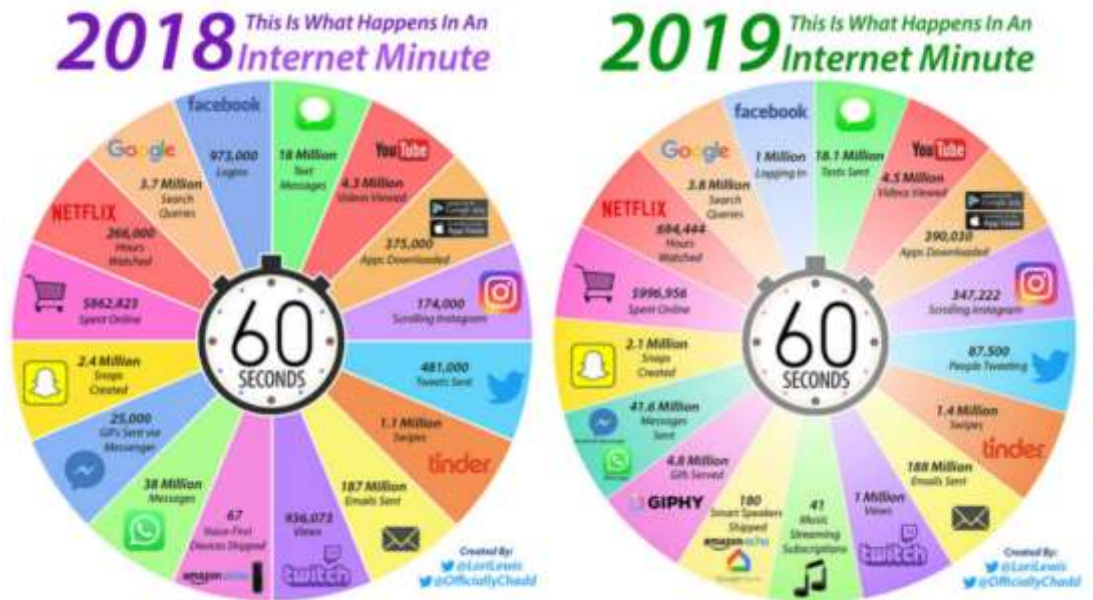
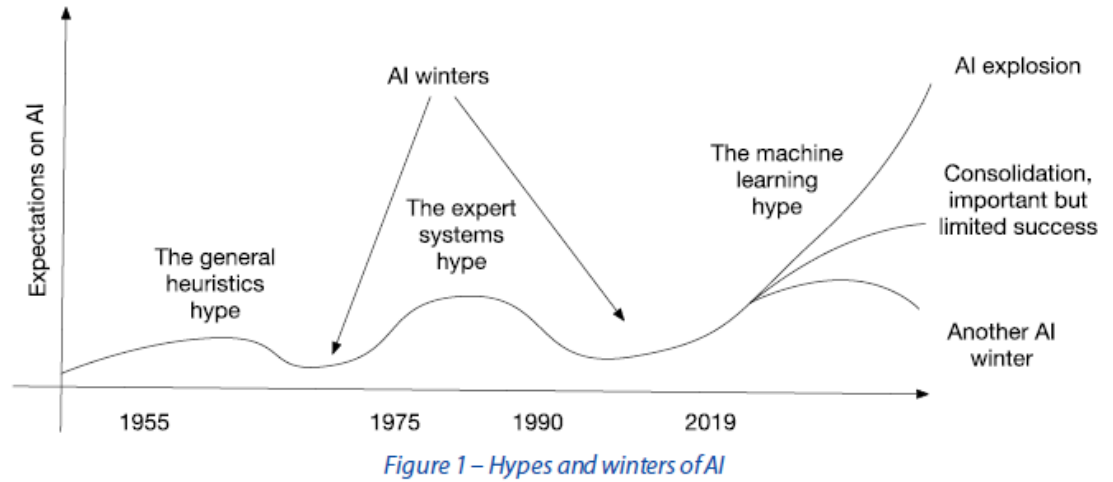
**STUDY**

Panel for the Future of Science and Technology

---

EPRS | European Parliamentary Research Service  
Scientific Foresight Unit (STDA)  
PE 641.530 – June 2020

EN





В докладе отмечается важность обсуждения и понимания всех типов угроз ИИ до начала его повсеместного развертывания, а также сертификации безопасности систем ИИ.

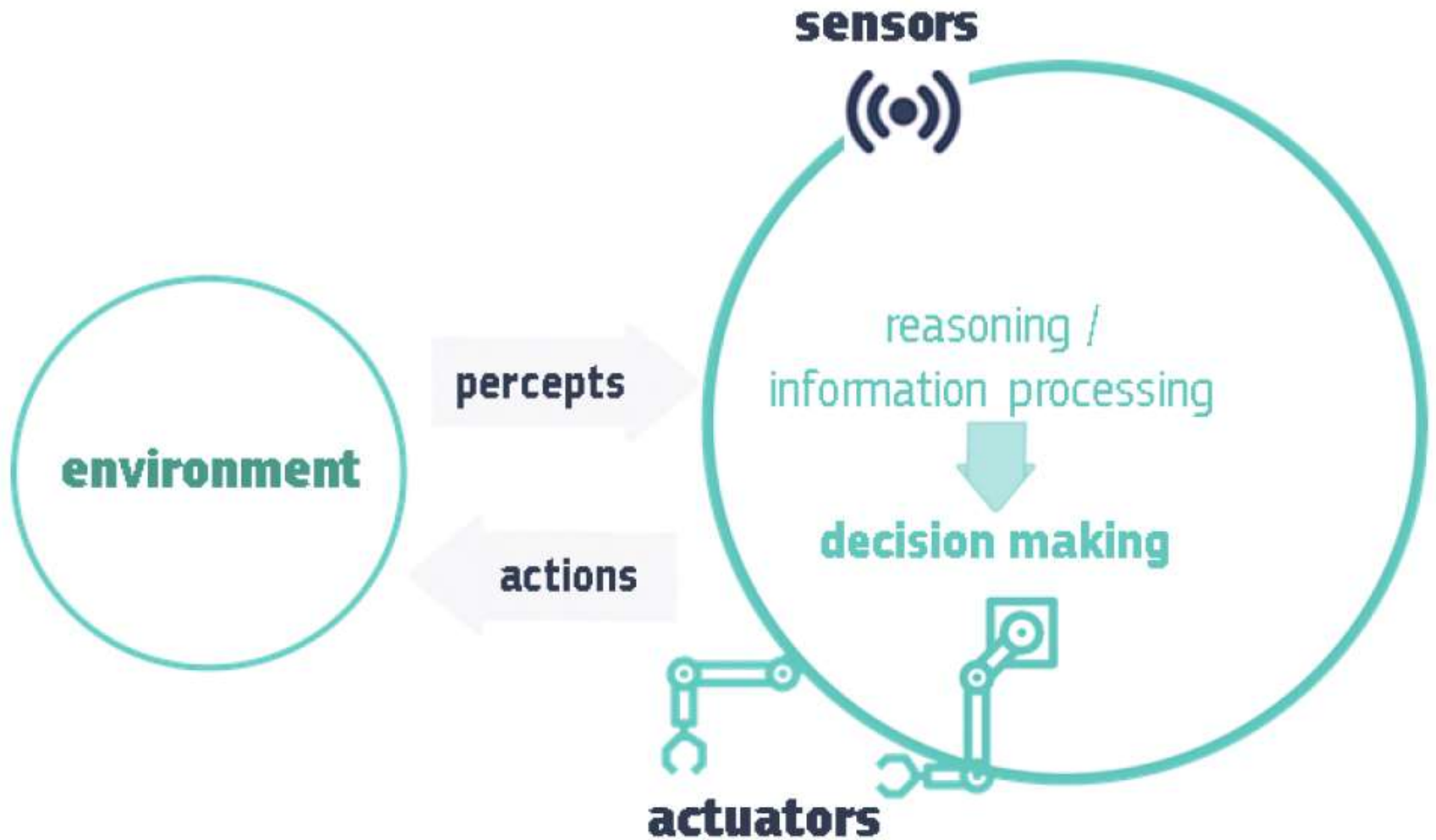
Среди основных угроз в сфере ИИ называются следующие:

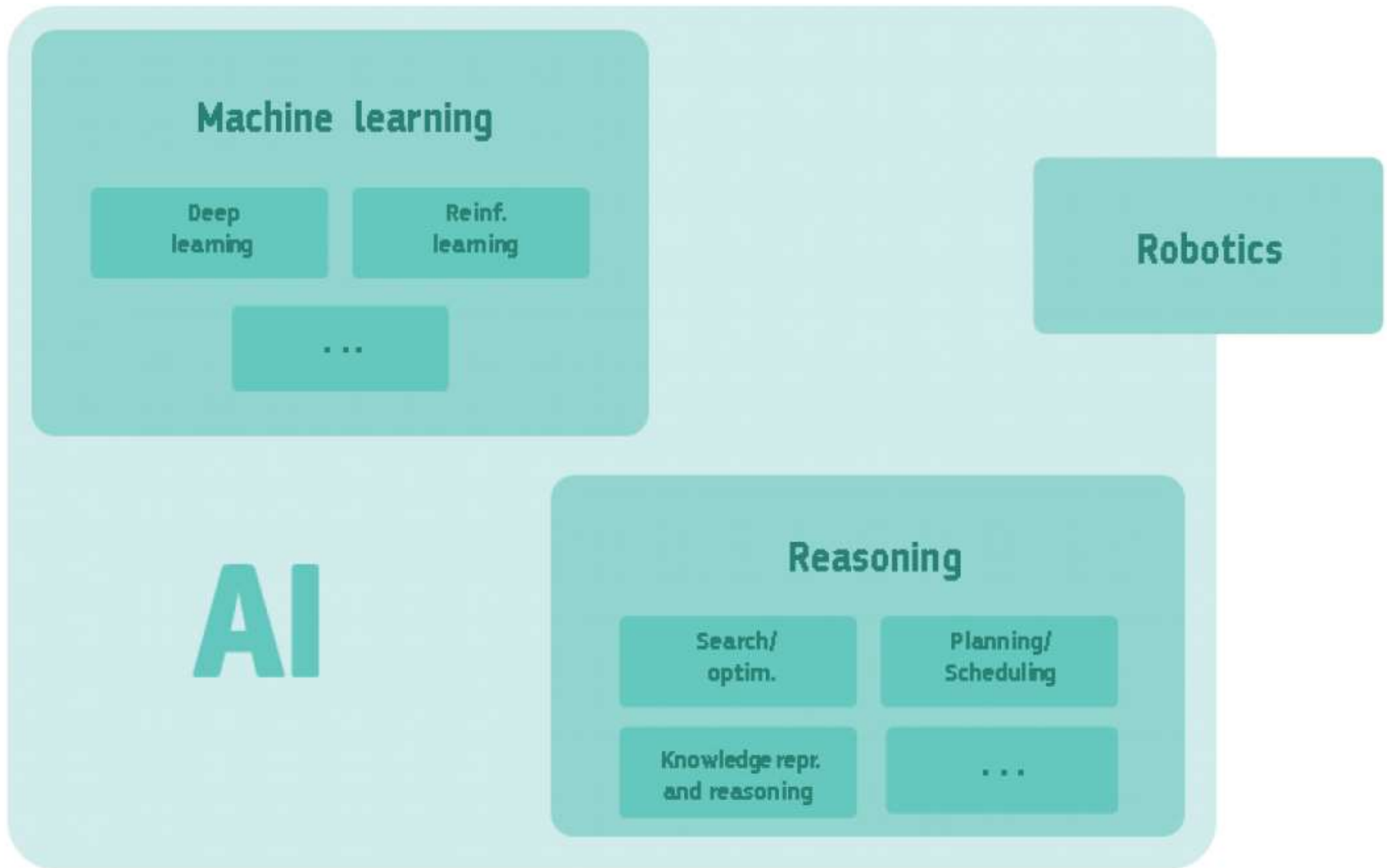
- кража или подделка, повреждение больших данных, используемых для обучения ИИ;
- атаки на промышленность и критическую инфраструктуру иностранных государств через взлом систем ИИ в целях сбора разведанных или нанесения прямого ущерба;
- подделка изображений и видео (deep fake), иные применения ИИ в преступных целях;
- инструмент для вторжения в частную жизнь.



EDPS и AEPD опубликовали совместно подготовленный обзор 10 распространенных заблуждений о машинном обучении (ML):

1. Корреляция предполагает причинность
2. При разработке ML-систем чем больше разнообразие данных, тем лучше
3. ML нуждается в полностью безошибочных обучающих наборах данных
4. Разработка ML-систем требует больших хранилищ данных или совместного использования наборов данных из разных источников
5. ML-модели автоматически улучшаются с течением времени
6. Автоматические решения, принимаемые алгоритмами ML, не могут быть объяснены
7. Принцип прозрачности в ML нарушает интеллектуальную собственность и непонятна пользователю
8. ML-системы менее подвержены человеческим предубеждениям
9. ML-системы могут точно предсказывать будущее
10. Люди способны предвидеть возможные результаты, которые ML-систем могут продуцировать из персональных данных



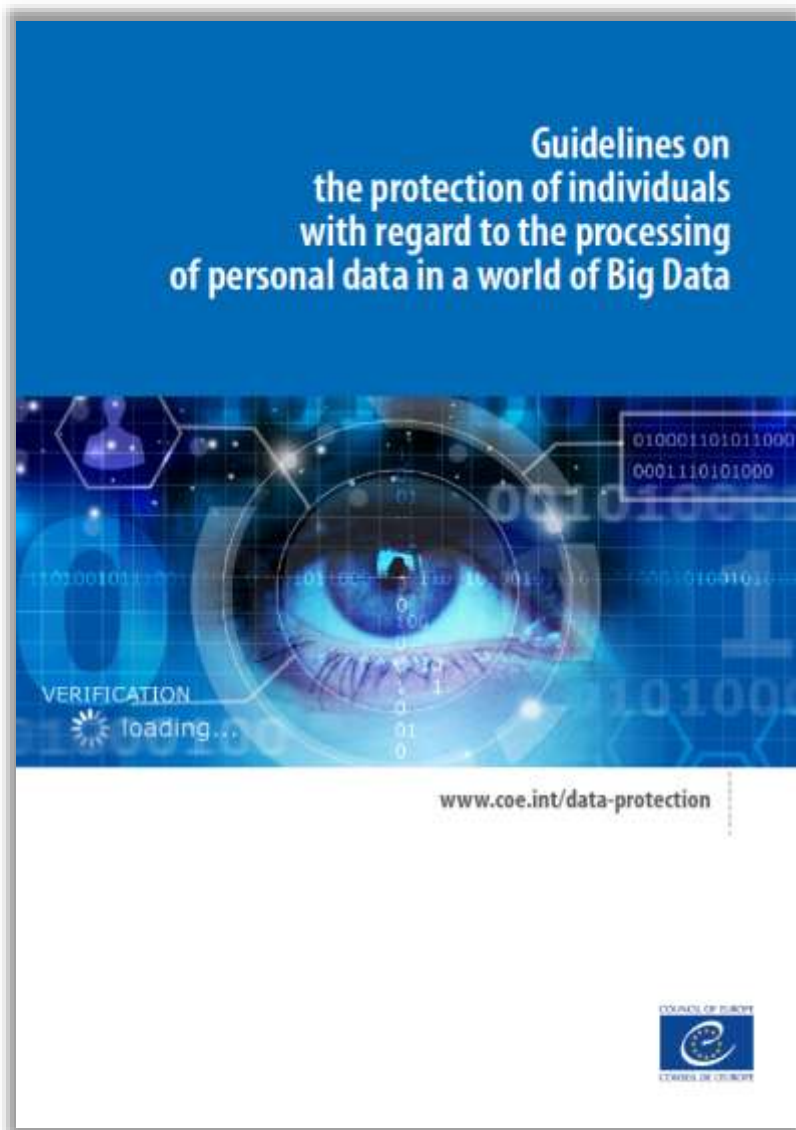


## Белая книга по искусственному интеллекту - европейский подход к совершенству и доверию



## On Artificial Intelligence - A European approach to excellence and trust

Европейская комиссия 19.02.2020 опубликовала «Белую книгу» по искусственному интеллекту, в которой описывается доктринальный подход ЕС к использованию и регулированию ИИ. В документе указывается, что ИИ быстро развивается и способен улучшить здравоохранение, повысить эффективность ведения сельского хозяйства, смягчить последствия изменения климата, повысить эффективность производственных систем посредством профилактического обслуживания, упрочить безопасность общества. В то же время ИИ влечет за собой ряд потенциальных рисков, таких как непрозрачное принятие решений, дискриминация по признаку пола или других признаков, вторжение в частную жизнь или использование в преступных целях.



### Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data

В январе 2019 года Консультативный комитет «Конвенции 108» Совета Европы (Council of Europe) опубликовал Руководство T-PD(2017)01, посвященное вопросам защиты физических лиц при обработке персональных данных при использовании технологий обработки больших данных.

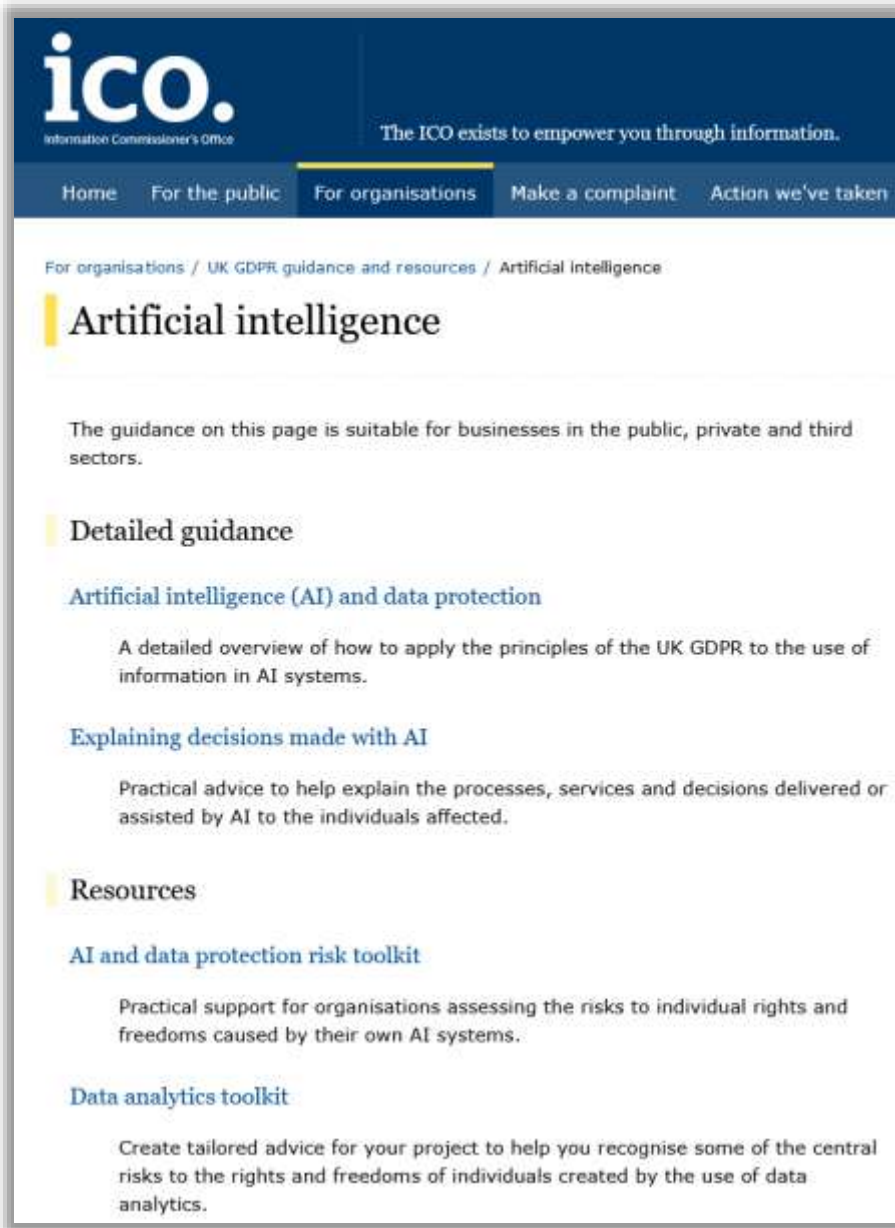
В Руководстве описываются меры, которые контролеры и обработчики должны принимать для предотвращения потенциального негативного воздействия использования больших данных на человеческое достоинство, права человека и основные индивидуальные и коллективные свободы, в частности в отношении защиты персональных данных.





### Big data, artificial intelligence, machine learning and data protection

Исследование, отражающее взгляды Управления уполномоченного по делам информации Соединенного Королевства (Information Commissioner's Office), о влиянии таких технологий обработки данных как большие данные, искусственный интеллект и машинное обучение на различные аспекты защиты персональных данных и приватности.



The screenshot shows the ICO website's page for Artificial Intelligence guidance. The header features the ICO logo and the tagline "The ICO exists to empower you through information." Below the header is a navigation menu with links for Home, For the public, For organisations (which is highlighted), Make a complaint, and Action we've taken. The main content area has a breadcrumb trail: "For organisations / UK GDPR guidance and resources / Artificial Intelligence". The main heading is "Artificial intelligence". A sub-heading states: "The guidance on this page is suitable for businesses in the public, private and third sectors." Below this are several sections:

- Detailed guidance**
  - Artificial intelligence (AI) and data protection**

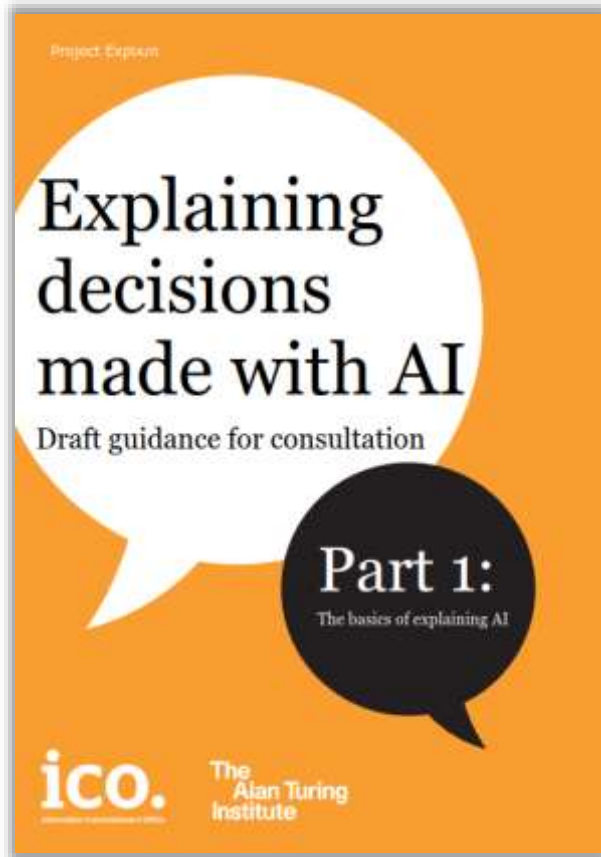
A detailed overview of how to apply the principles of the UK GDPR to the use of information in AI systems.
  - Explaining decisions made with AI**

Practical advice to help explain the processes, services and decisions delivered or assisted by AI to the individuals affected.
- Resources**
  - AI and data protection risk toolkit**

Practical support for organisations assessing the risks to individual rights and freedoms caused by their own AI systems.
  - Data analytics toolkit**

Create tailored advice for your project to help you recognise some of the central risks to the rights and freedoms of individuals created by the use of data analytics.

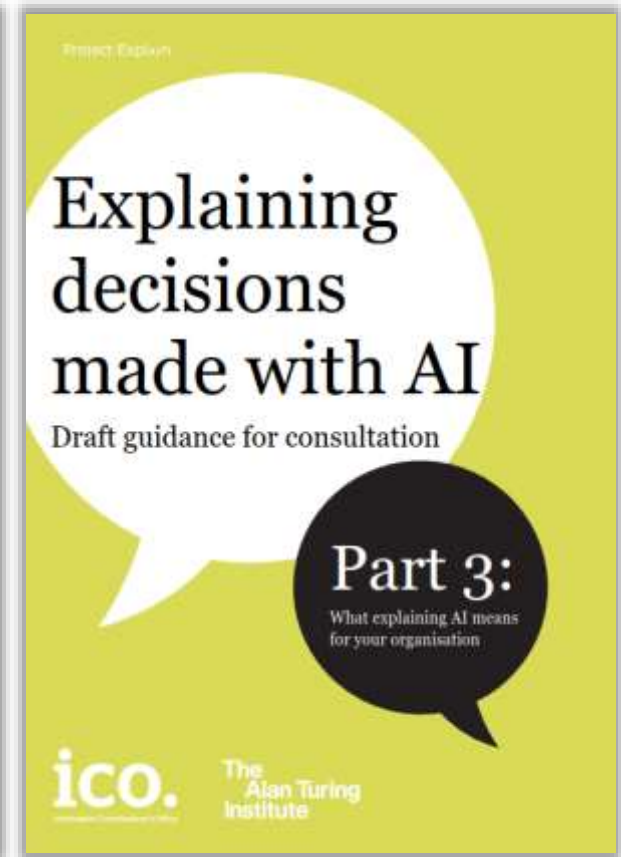
Управление уполномоченного по делам информации Соединенного Королевства (Information Commissioner's Office) подготовило обновленную версию руководства по оценке рисков защиты данных в ИИ, включая рекомендации по организационным и техническим мерам по снижению рисков, которые ИИ представляет для отдельных лиц. Документ также предоставляет надежную методологию для аудита систем ИИ и обеспечения ими справедливой и законной обработки персональных данных.



**Part 1: The basics of explaining AI**

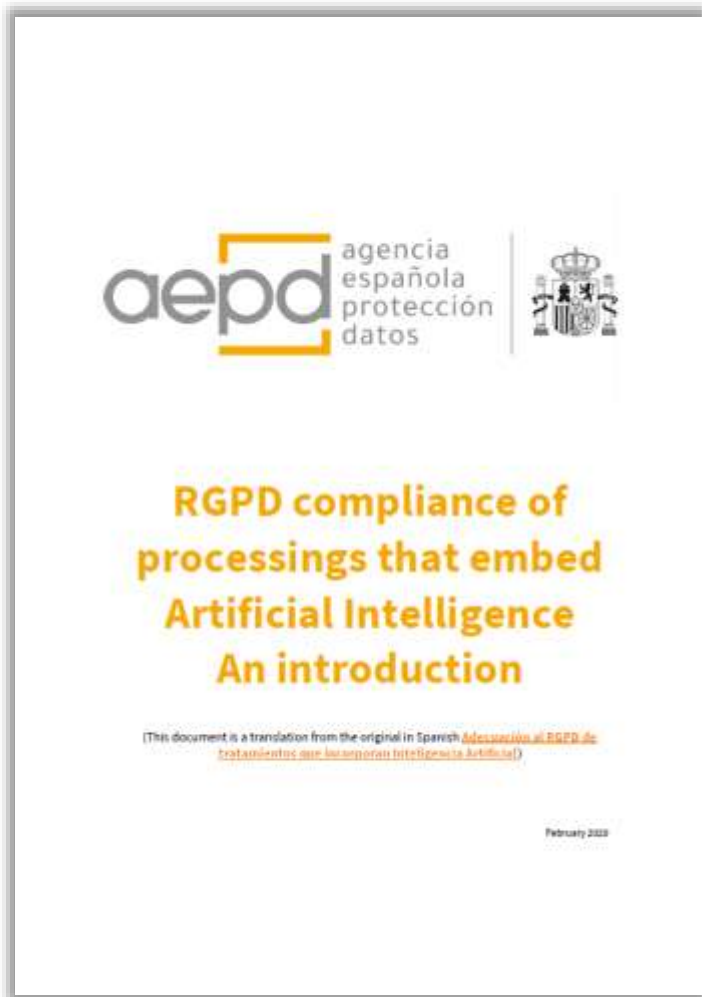


**Part 2: Explaining AI in practice**

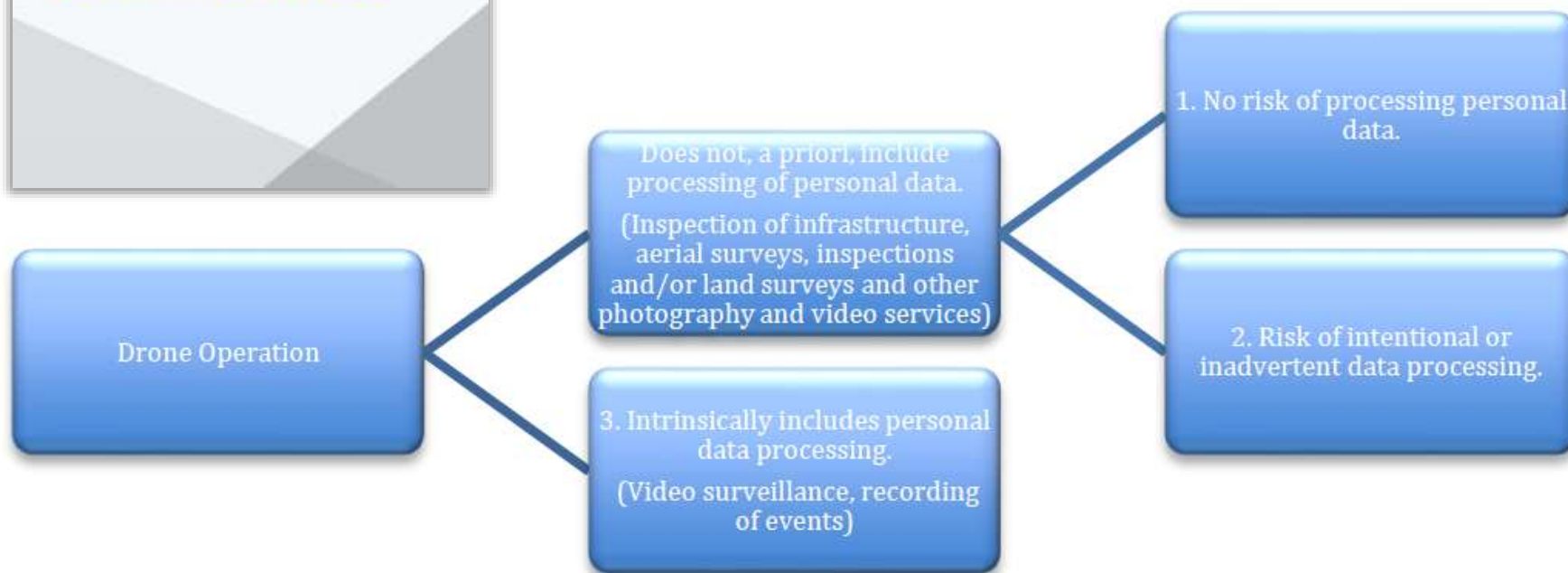


**Part 3: What explaining AI means for your organisation**

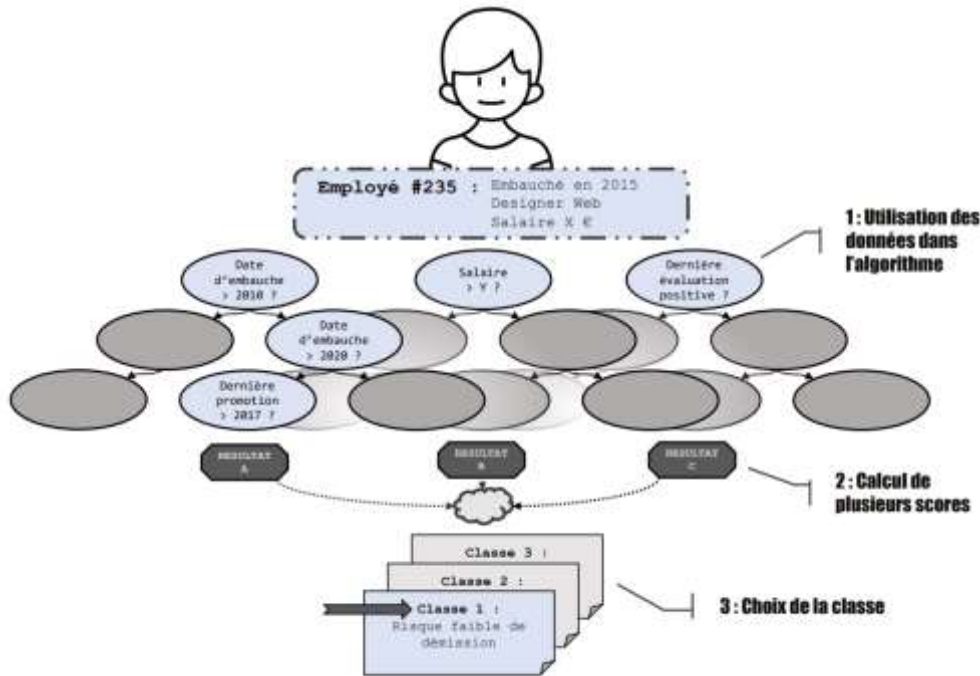
## Руководство AEPD по использованию технологий ИИ в контексте требований GDPR



- I. INTRODUCTION TO THE AI FRAMEWORK AND DATA PROTECTION
  - A. AI Techniques
  - B. Data processing by means of AI solutions
  - C. Data protection and ethical dimension
  - D. GDPR definitions
  - E. Life cycle of an AI solution
  - F. Personal data processing by means of AI
  - G. Assessment of AI-based solutions
  - H. Short summary of obligations lay down by the GDPR
- II. ROLES, RELATIONSHIPS AND RESPONSABILITIES
- III. COMPLIANCE
  - A. Lawfulness and limited purpose
    - Legitimate interest
    - Special categories
    - Processing for compatible purposes
  - B. Information
    - Relevant information on the implemented logic
  - C. General aspects related to the exercise of rights
  - D. Right to access
  - E. Right to erasure
    - Limitations to erasure
  - F. Blocking of data
  - G. Right to rectification
  - H. Portability
  - I. Decision-making based on automated processing
- IV. PRIVACY RISKS MANAGEMENT
  - A. Risk assessment
  - B. Privacy Impact Assessment-(PIA)
  - C. Transparency
    - During training
    - Certification
    - Automated decisions and profiling
    - Data controller personnel
    - The Data Protection Officer as a tool for transparency
  - D. Accuracy
    - Factors affecting accuracy
    - Biometric information
    - Profiling combination
    - Verification vs. Validation
    - Accuracy assessment as continuous process
  - E. Minimisation
    - Training data
    - Minimisation techniques
    - Extent of the data categories in an AI-based solution
    - Extent of the training set
    - Personal data in the AI-based solution
  - F. Security
    - Specific threats in AI components
    - Logs or activity records
  - G. Assessment of the proportionality and the need for such processing
  - H. Audit
- V. INTERNATIONAL TRANSFERS
- VI. CONCLUSIONS
- VII. REFERENCES
- VIII. ANNEX: CURRENT AI-BASED SERVICES



## Руководство CNIL по соблюдению GDPR в отношении ИИ и инструменты для самооценки



Французский орган по защите данных (CNIL) 05.04.2022 опубликовал руководство и инструменты для самооценки по соблюдению требований GDPR при использовании технологий искусственного интеллекта («ИИ»). Примечательно, что опубликованные материалы предназначены для трех разных аудиторий: широкой слоев населения; контролеров и процессоров; специалистов по ИИ.

<https://www.cnil.fr/fr/intelligence-artificielle/ia-comment-etre-en-conformite-avec-le-rgpd>

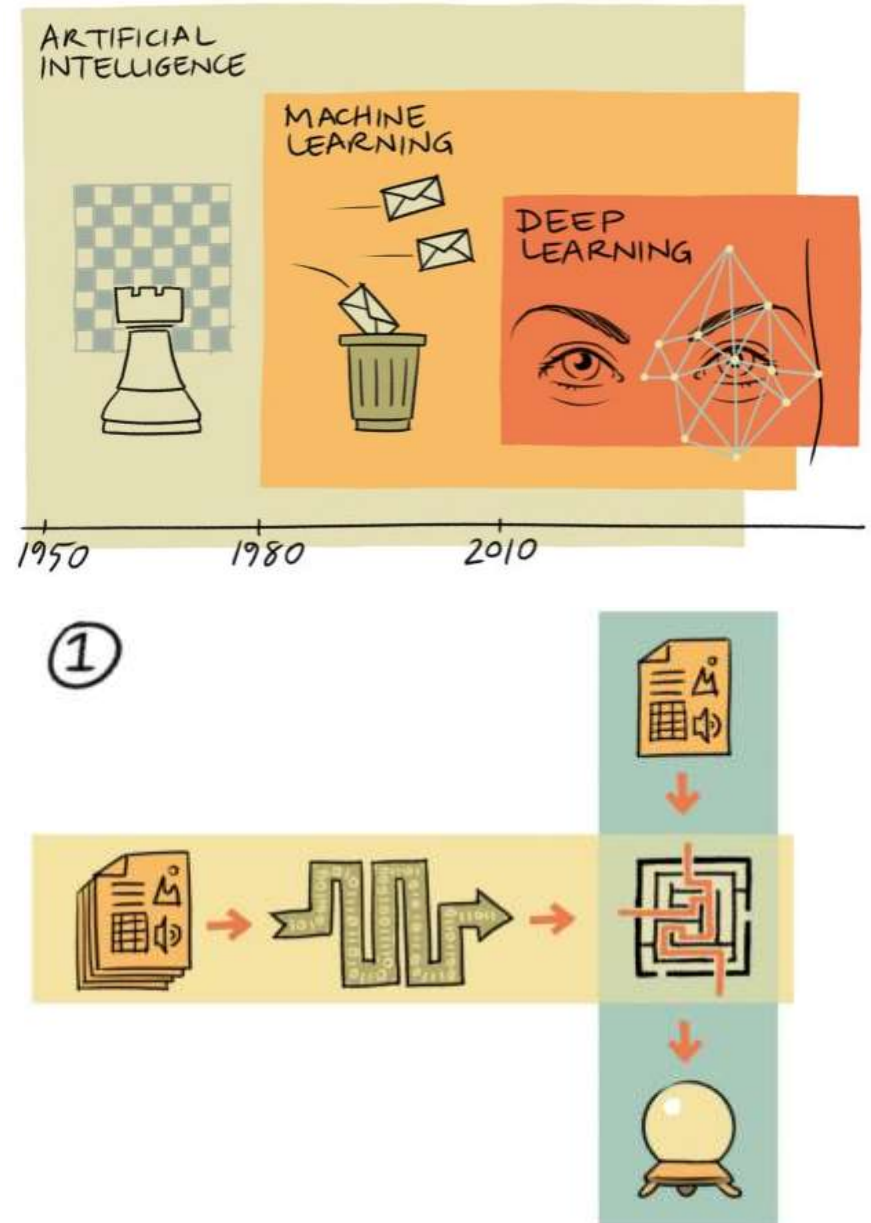
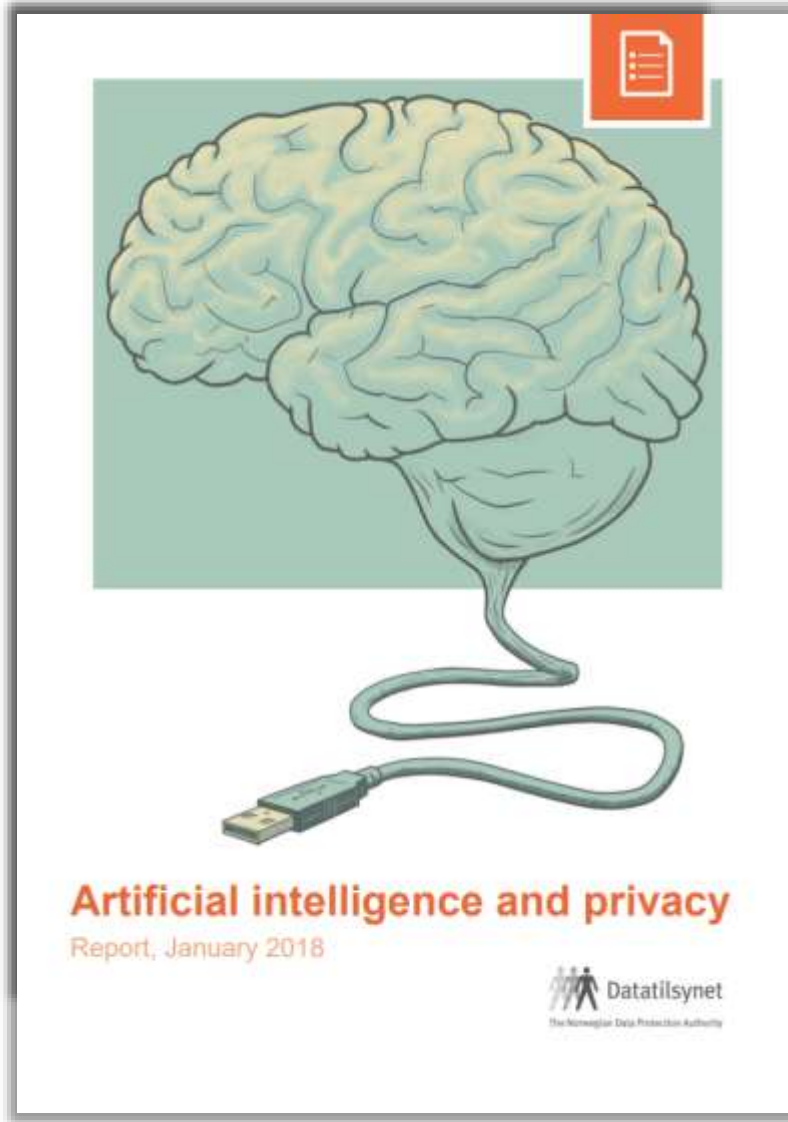
<https://www.cnil.fr/fr/intelligence-artificielle/guide/developper-et-entrainer-un-algorithme>

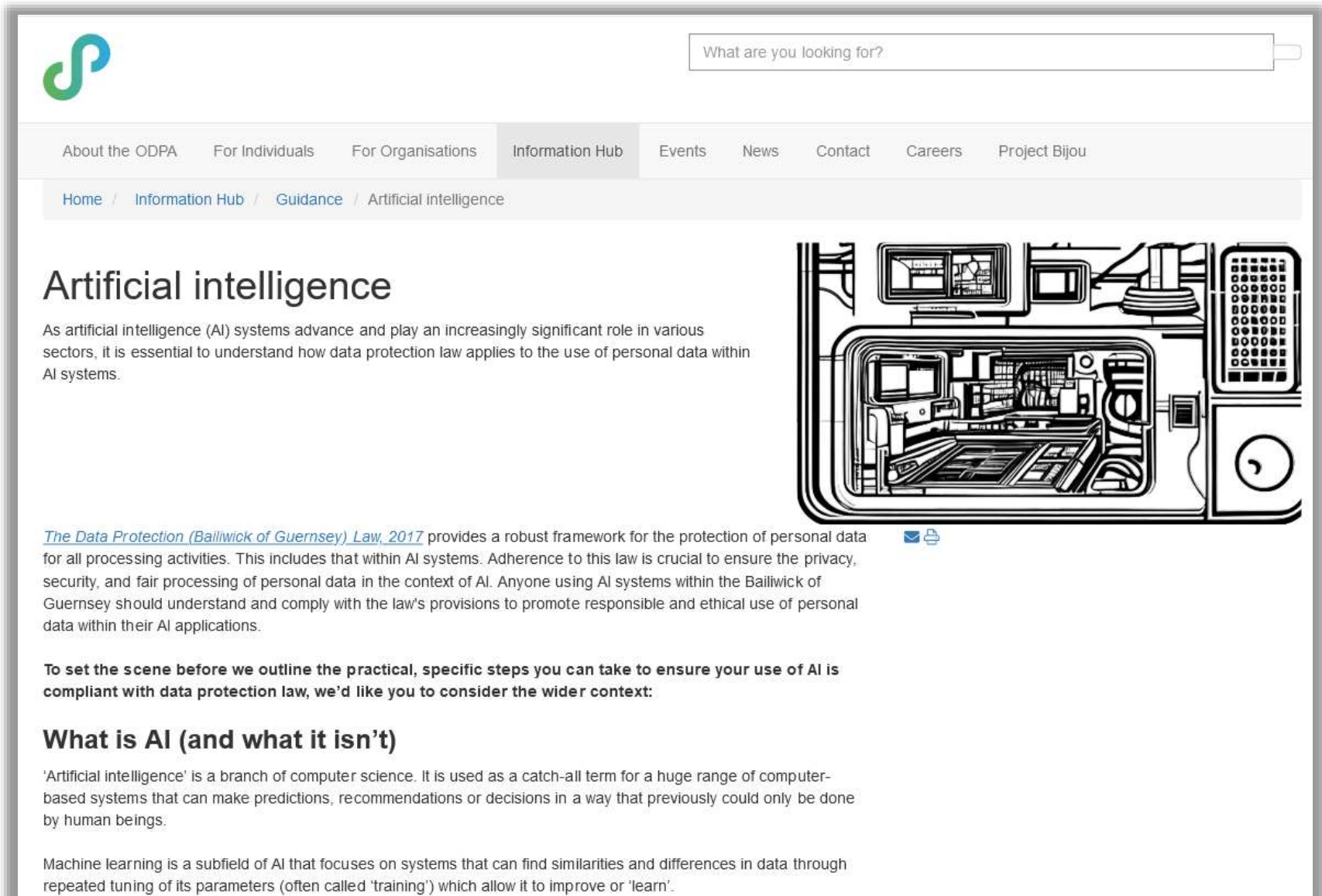
<https://www.cnil.fr/fr/intelligence-artificielle/guide/utiliser-un-systeme-dia-en-production>

<https://www.cnil.fr/fr/intelligence-artificielle/guide>

<https://www.cnil.fr/fr/intelligence-artificielle-ia>

# Руководство норвежского Datatilsynet по использованию технологий ИИ в контексте требований GDPR

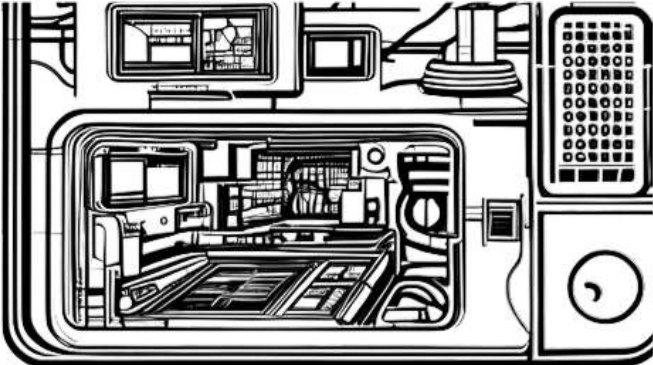




The screenshot shows the ODPA Information Hub website. At the top left is the ODPA logo, a stylized 'D' and 'P' in green and blue. To the right is a search bar with the placeholder text "What are you looking for?". Below the search bar is a navigation menu with links: "About the ODPA", "For Individuals", "For Organisations", "Information Hub" (which is highlighted), "Events", "News", "Contact", "Careers", and "Project Bijou". Below the navigation menu is a breadcrumb trail: "Home / Information Hub / Guidance / Artificial intelligence".

# Artificial intelligence

As artificial intelligence (AI) systems advance and play an increasingly significant role in various sectors, it is essential to understand how data protection law applies to the use of personal data within AI systems.



[The Data Protection \(Bailiwick of Guernsey\) Law, 2017](#) provides a robust framework for the protection of personal data for all processing activities. This includes that within AI systems. Adherence to this law is crucial to ensure the privacy, security, and fair processing of personal data in the context of AI. Anyone using AI systems within the Bailiwick of Guernsey should understand and comply with the law's provisions to promote responsible and ethical use of personal data within their AI applications.

**To set the scene before we outline the practical, specific steps you can take to ensure your use of AI is compliant with data protection law, we'd like you to consider the wider context:**

### What is AI (and what it isn't)

'Artificial intelligence' is a branch of computer science. It is used as a catch-all term for a huge range of computer-based systems that can make predictions, recommendations or decisions in a way that previously could only be done by human beings.

Machine learning is a subfield of AI that focuses on systems that can find similarities and differences in data through repeated tuning of its parameters (often called 'training') which allow it to improve or 'learn'.



# Этика подключенных и автоматизированных транспортных средств (включая рекомендации по privacy)



## ETHICS of Connected and Automated Vehicles

The European Commission's strategy on Cooperative, Connected and Automated Mobility (CCAM) aims to make Europe a world leader in the development and deployment of Connected and Automated Vehicles (CAVs).

Expectations are high. These vehicles can:

- bring down road fatalities to near zero
- increase accessibility of mobility services
- help to reduce harmful emissions from transport by making traffic more efficient

To reap the full benefits of these vehicles, many challenges have to be addressed: societal, technical, regulatory, economic, environmental and ethical.

**New technologies do not appear out of nowhere: they are imagined by people and built with purpose.**  
EU values and principles need to be integrated at the core of these new technologies to ensure their ethical use and positive impact. Our ability to reach a just, sustainable and inclusive society depends on them.

To tackle ethical issues, the Commission formed in 2019 an independent Expert Group to advise on specific ethical issues raised by driverless mobility. The Expert Group focused on three themes:

**ROAD SAFETY, RISK, DILEMMAS:**

- Safety benefits and improvements of CAVs should comply with basic ethical and legal principles; they should be publicly demonstrable, monitored and updated through solid and shared scientific research, and continuously adjusted to the needs of all road users.

**DATA AND ALGORITHM ETHICS: PRIVACY, FAIRNESS, EXPLAINABILITY:**

- Artificial Intelligence (AI) and automated systems used in CAVs should be explainable and transparent to empower users and to protect their data.
- This should be reflected through rules and regulations that take into account the fact-changing nature of CAV technologies (especially AI and big data) and favour inclusive deliberation at all levels.

**RESPONSIBILITY:**

- Responsibilities should be clearly attributed and shared, going beyond blame and compensation in case of a collision. No single person or system can be held solely accountable.
- From inception to use, best practices promoting ethical responsibility must be fostered and shared. This way humans can remain accountable to users, instead of complex systems.

Research and Innovation

20 RECOMMENDATIONS are available to support researchers, policymakers, manufacturers and deployers in the safe and responsible transition towards CAVs.

1. Ensure that CAVs reduce physical harm to persons.
2. Prevent unsafe use by inherently safe design.
3. Define clear standards for responsible open road testing.
4. Consider revision of traffic rules to promote safety of CAVs and investigate exceptions to non-compliance with existing rules by CAVs.
5. Redress inequalities in vulnerability among road users.
6. Manage dilemmas by principles of risk distribution and shared ethical principles.
7. Safeguard informational privacy and informed consent.
8. Enable user choice, seek informed consent options and develop related best practice industry standards.
9. Develop measures to foster protection of individuals at group level.
10. Develop transparency strategies to inform users and pedestrians about data collection and associated rights.
11. Prevent discriminatory differential service provision.
12. Audit CAV algorithms.
13. Identify and protect CAV relevant high-value datasets as public and open infrastructural resources.
14. Reduce opacity in algorithmic decisions.
15. Promote data, algorithmic, AI literacy and public participation.
16. Identify the obligations of different agents involved in CAVs.
17. Promote a culture of responsibility with respect to the obligations associated with CAVs.
18. Ensure accountability for the behaviour of CAVs (duty to explain).
19. Promote a fair system for the attribution of moral and legal culpability for the behaviour of CAVs.
20. Create fair and effective mechanisms for granting compensation to victims of crashes or other accidents involving CAVs.

Research and Innovation (R&I) on CCAM is already taking place at local, national and EU-level. From 2014 to 2020, around EUR 350 million were allocated to support projects through Horizon 2020.

Under the next EU research and innovation Framework programme, **Horizon Europe**, R&I on CCAM will remain a key priority. By leveraging the digitalisation of transport with smart, shared, connected and automated mobility systems and together with the European Green Deal, Europe is set to lead the twin digital and green transition towards becoming the world's first climate-neutral continent by 2050.

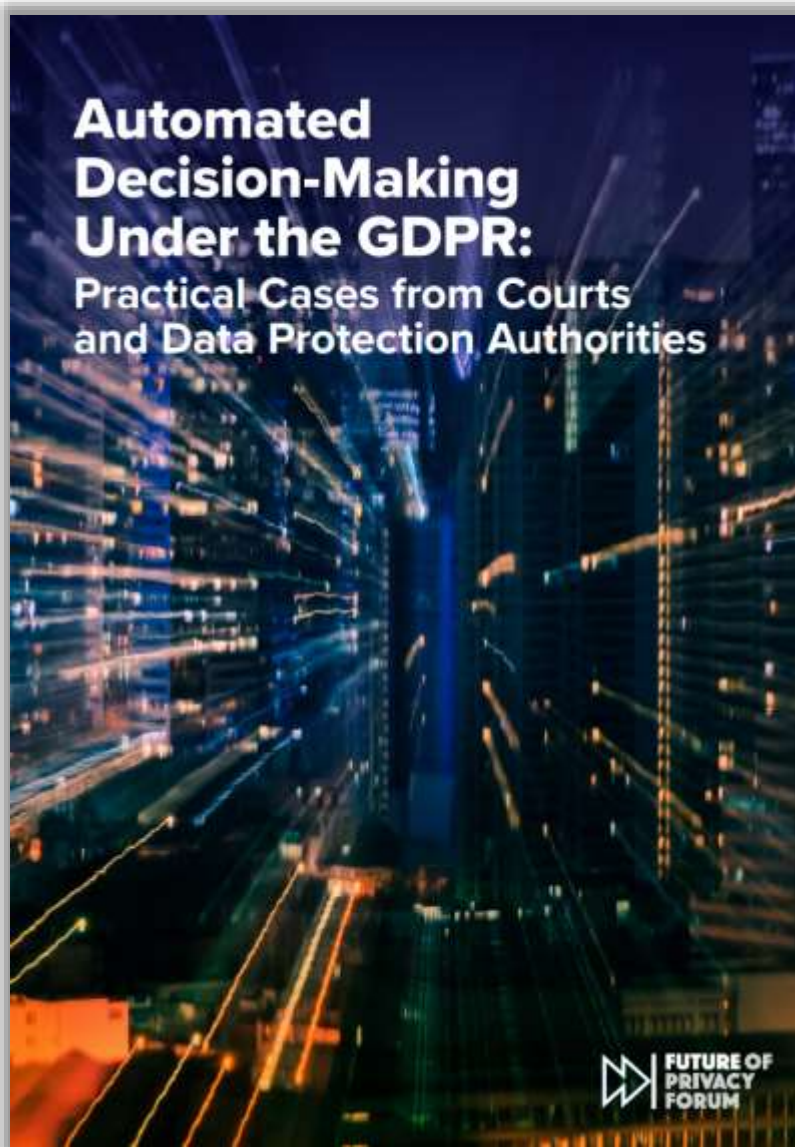
An upcoming **European Partnership** will bring together the actors of the complex cross-sectoral value chain of CCAM to develop and implement a shared, coherent and long-term European R&I policy that will benefit EU citizens and support EU industries.

The recommendations of this Expert Group report will be key in defining R&I priorities related to societal and ethical issues. Acceptance and trust by users and society, will have to be nurtured every step of the way.

To read the Expert Group report on the Ethics of Connected and Automated Vehicles, visit <https://ec.europa.eu/00062mz>

© European Union, 2020  
 Free: ISBN 978-92-76-22934-6, doi:10.27771948473, 43-02-20-075-04-X  
 PDF: ISBN 978-92-76-22944-3, doi:10.2777193884, 43-02-20-075-04-X

## Автоматическое принятие решений в соответствии с GDPR: практические примеры из практики судов и органов по защите данных



<b>Background and Overview</b>	<b>2</b>
<b>1. The Fundamentals of Article 22 GDPR</b>	<b>5</b>
1.1 ADM provisions have been enshrined in data protection laws since the 1970s	6
1.2 The EDPB interprets Article 22 as an a priori prohibition on engaging in qualifying ADM	7
1.3 There are three conditions that trigger the applicability of Article 22 GDPR	8
1.4 Only legal obligations, contract and consent can justify qualifying ADM	9
1.5 Human intervention, the right to be heard and contestability must be ensured for qualifying ADM	10
1.6 The rest of the GDPR applies to ADM and qualifying ADM, regardless of Article 22 conditions	13
a. General data protection principles, including fairness, apply to all ADM	13
b. Personal data processing underlying ADM and profiling require a lawful ground for processing	15
c. General transparency requirements apply to ADM and profiling, regardless of whether it is qualifying ADM or not	18
d. DPIAs are always required for qualifying ADM in some EU Member States	25
<b>2. Assessing the Threshold that Triggers Article 22: Case-Law</b>	<b>28</b>
2.1 "Solely automated processing" can sometimes include human involvement	28
2.2 "Legal or similarly significant effects" require a multi-dimensional, case-by-case analysis	35
<b>3. ADM and the GDPR Case-Law in Specific Scenarios: Workplace — Facial Recognition — Credit Scoring</b>	<b>39</b>
3.1 ADM in the workplace often interacts with labor rights	39
3.2 Facial Recognition is broadly regulated by the GDPR, beyond Article 22	41
3.3 Credit Scoring is justified on "contractual necessity" only if it relies on relevant information	45
<b>Conclusion</b>	<b>48</b>
<b>Annex 1 — List of Cases</b>	<b>50</b>
<b>Endnotes</b>	<b>55</b>

## Анализ CNIL этических, технических и юридических вопросов, связанных с голосовыми помощниками

**1 - Maintaining positive friction:** rather than focusing on implementing an absolutely seamless user experience, take advantage of moments of interaction (i.e. moments of choice, of settings, requiring the user's attention) to present the reality of data processing to users in an adapted manner (see box on page 69).

**2 - Preferring the local to the remote:** as far as possible, implement data processing modalities and capacities directly in the devices, which gives the user a good level of control over them and is a factor of confidence and acceptability.

**3 - Ensuring the means of control:** enable the user to understand and control the uses made of his/her data and to configure the device's operation according to his/her choices.

**4 - Adapting to the voice medium:** relying on audio-only interfaces raises significant challenges in terms of presenting information to the user, obtaining consent or implementing means of control. It is therefore necessary to reflect on the means to be deployed.

As presented in Chapter III *Use cases: GDPR in practice* (page 46), the use of a voice assistant must meet data protection requirements. Specifically, it is necessary to ensure that all the key principles outlined in the GDPR are met (see *The key concepts of GDPR*, page 48):





**DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE**

40<sup>th</sup> International Conference of Data Protection and Privacy Commissioners

Tuesday 23<sup>rd</sup> October 2018, Brussels

AUTHORS:

- Commission Nationale de l'Informatique et des Libertés (CNIL), France
- European Data Protection Supervisor (EDPS), European Union
- Garante per la protezione dei dati personali, Italy

CO-SPONSORS:

- Agencia de Acceso a la Información Pública, Argentina
- Commission d'accès à l'information, Québec, Canada
- Datatilsynet (Data Inspectorate), Norway
- Information Commissioner's Office (ICO), United Kingdom
- Préposé fédéral à la protection des données et à la transparence, Switzerland
- Data protection Authority, Belgium
- Privacy Commissioner for Personal Data, Hong-Kong
- Data protection Commission, Ireland
- Data Protection Office, Poland
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Mexico
- National Authority for Data Protection and Freedom of Information, Hungary
- Federal Commissioner for Data Protection and Freedom of Information, Germany
- Office of the Privacy Commissioner (OPC), Canada
- National Privacy Commission, Philippines

## Declaration on ethics and data protection in artificial intelligence

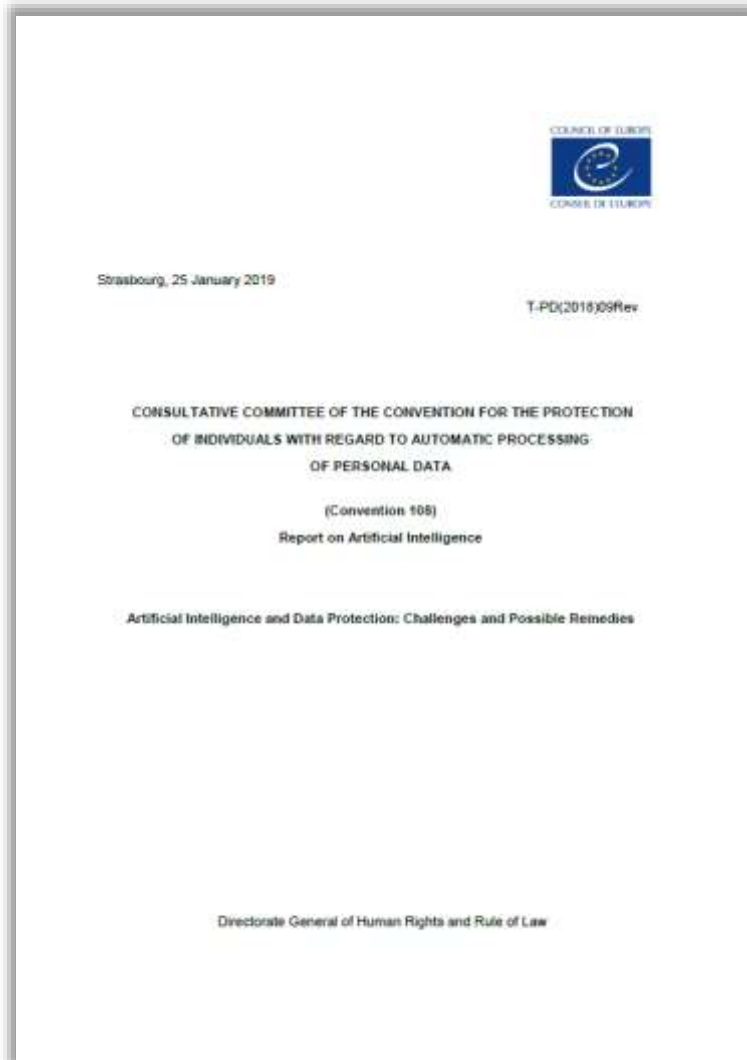
Декларация об этике и защите данных в системах искусственного интеллекта, принятая 23.10.2018 на 40-й Международной конференции уполномоченных по защите данных и конфиденциальности (International Conference of Data Protection and Privacy Commissioners).

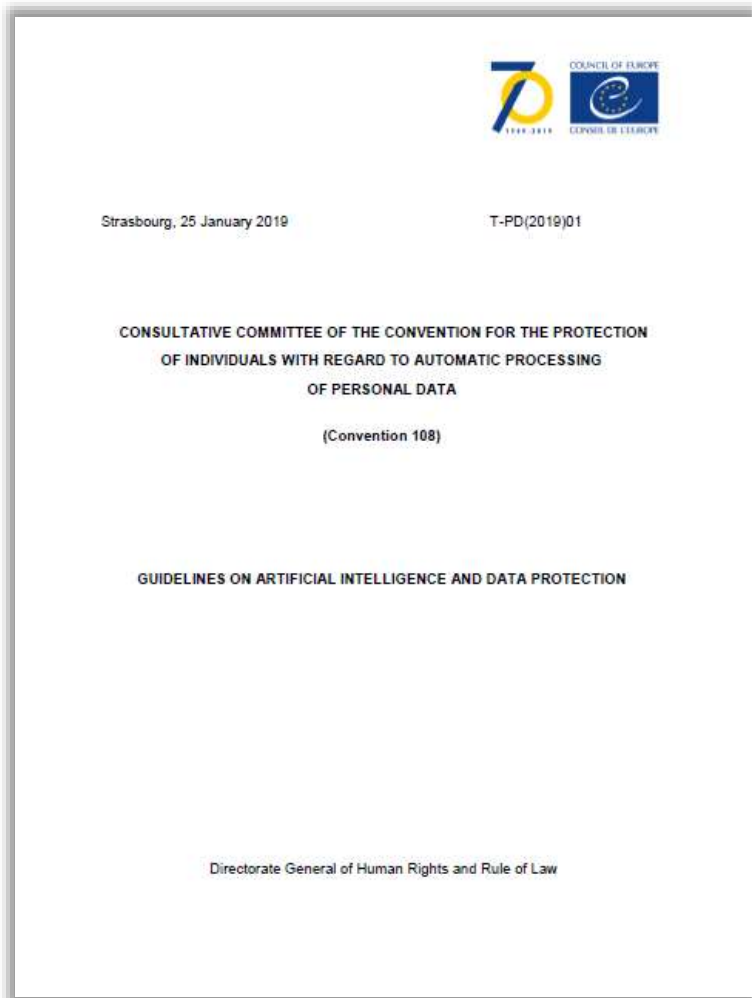
Учреждена постоянно действующая Рабочая группа по этике и защите данных в искусственном интеллекте (working group on Ethics and Data Protection in Artificial Intelligence).

## Отчет от СЕ «Искусственный интеллект и защита данных: вызовы и возможные ответы на них»

### Artificial Intelligence and Data Protection: Challenges and Possible Remedies

В январе 2019 года Консультативный комитет «Конвенции 108» Совета Европы (Council of Europe) опубликовал Отчет T-PD(2018)09Rev, посвященный выявленным при использовании технологий искусственного интеллекта для обработки персональных данных правовым проблемам и способам их решения.





### Guidelines on artificial intelligence and data protection

В январе 2019 года Консультативный комитет «Конвенции 108» Совета Европы (Council of Europe) опубликовал Руководство T-PD(2019)01, которое даёт определённое представление о контурах европейского правового регулирования использования технологий искусственного интеллекта (ИИ) для обработки персональных данных.

Технологии ИИ не только представляют потенциальную угрозу для неприкосновенности частной жизни, но и часто сознательно проектируются для профилирования людей. Одновременно европейское законодательство и без того является очень жёстким, и оно потенциально способно очень существенно замедлить развитие ИИ в Европе.

Руководство направлено на то, чтобы помочь создателям политик, разработчикам искусственного интеллекта (ИИ), производителям продуктов и поставщикам услуг в обеспечении того, чтобы ИИ-приложения не подрывали право на защиту персональных данных.



### Ethics Guidelines for Trustworthy AI

В апреле 2019 года было опубликовано Руководство, подготовленное Группой экспертов высокого уровня по искусственному интеллекту (AI HLEG), созданной при Европейской комиссии. Эта независимая экспертная группа была создана Европейской комиссией в июне 2018 года в рамках [стратегии ИИ](#), объявленной ранее в этом году.

Руководство не похоже на «Три закона робототехники» Исаака Азимова. Оно не предлагает быстрых, моральных рамок, которые помогут контролировать потенциально опасных роботов. Вместо этого Руководство анализирует различные этические аспекты использования ИИ, которые будут влиять на общество, поскольку все больше организаций планирует использовать ИИ в таких отраслях как здравоохранение, образование и конечное потребление.

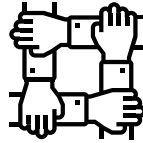
Руководство не имеет обязательной юридической силы, но оно будет способствовать формированию в будущем европейского законодательства в области ИИ.

## 440 Признаки и качества «благонадежного и человеческого» ИИ



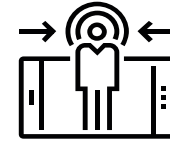
### Lawful

Respecting all applicable laws and regulations



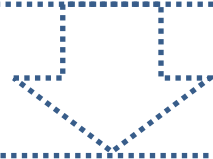
### Ethical

Respecting ethical principles and values



### Robust

Both from a technical perspective while taking into account its social environment



- ✓ Human agency and oversight
- ✓ Technical robustness and safety
- ✓ Privacy and Data governance
- ✓ Transparency
- ✓ Diversity, non-discrimination and fairness
- ✓ Societal and environmental well-being
- ✓ Accountability



## 441 Оценка благонадежного искусственного интеллекта



Группа экспертов высокого уровня по искусственному интеллекту (AI HLEG) представила Европейской комиссии свой окончательный проект документа по оценке степени благонадежности искусственного интеллекта. Базовые принципы, касающиеся конфиденциальности и управления данными, а также технической надежности и безопасности обработки данных, были представлены в виде списка контрольных вопросов (чек-листа), который призван оказать практическую помощь разработчикам и техническим специалистам в области ИИ.

Относительно требований по защите персональных данных в список включены вопросы об обеспечении соответствия GDPR, например, об осуществлении при разработке ИИ оценки воздействия на защиту данных (DPIA), а также оценки необходимости и пропорциональности обработки ИИ персональных данных.



**Datatilsynet**

**Å lykkes med åpenhet**


Åpenhet knyttet til kunstig intelligens er en vid paraply. Med en gang kunstig intelligens brukes på personopplysninger, stilles det regelverkskrav til åpenhet. Under paraplyen finner vi også etiske spørsmål og teknologiske problemstillinger rundt kommunikasjon og design. Vi har skrevet en erfaringsrapport om hvordan du bør informere om bruk av kunstig intelligens.

**Innledning**


Regelverket setter klare krav til åpenhet. Men det gir ikke sylskarpe grenser og en tydelig oppskrift på hvordan man skal være åpen. Det må gjøres egne vurderinger i hvert enkelt tilfelle. Nettopp derfor vier vi så god plass til eksemplene i denne rapporten, fordi vurderinger og tiltak i disse eksemplene fra virkeligheten kan ha overføringsverdi til andre som har lignende spørsmål.


Hva slags informasjon må man gi? Hvor detaljert må informasjonen være? Hvordan bør man informere? Og hvor og når bør informasjonen gis? Regelverket setter krav og gir brukeren rett til informasjon, men hvordan dette skal implementeres i praksis må vurderes fra sak til sak. Dette er ikke en komplett guide til alle sider av åpenhet ved bruk av kunstig intelligens. Men vi trekker frem noen sentrale sandkassediskusjoner vi tror kan ha nytteverdi for andre.

Норвежский орган по защите данных ("Datatilsynet") 21.12.2022 опубликовал отчет, призванного помочь организациям в информировании субъектов данных об использовании искусственного интеллекта ("ИИ"). В отчете изложены наиболее важные юридические требования, касающиеся прозрачности использования ИИ, и приведены конкретные примеры, предлагающие список действий для достижения прозрачности ИИ. Хотя нормативные акты устанавливают четкие требования к прозрачности, они не дают четкого рецепта, как быть прозрачным, поэтому в каждом отдельном случае необходимо проводить отдельную оценку. Чтобы люди были готовы принимать решения и делиться информацией с ИИ, они должны быть уверены в том, что решение работает для своей цели, обеспечивая при этом конфиденциальность.



Federal Office for Information Security





Whitepaper | May 2022

# Towards Auditable AI Systems

## From Principles to Practice

based on the 2nd international Workshop "Towards Auditable AI Systems", October 26<sup>th</sup> 2021, Fraunhofer Forum Digitale Technologien, Berlin, organized by the Federal Office for Information Security Germany, the TÜV-Verband and the Fraunhofer HHI

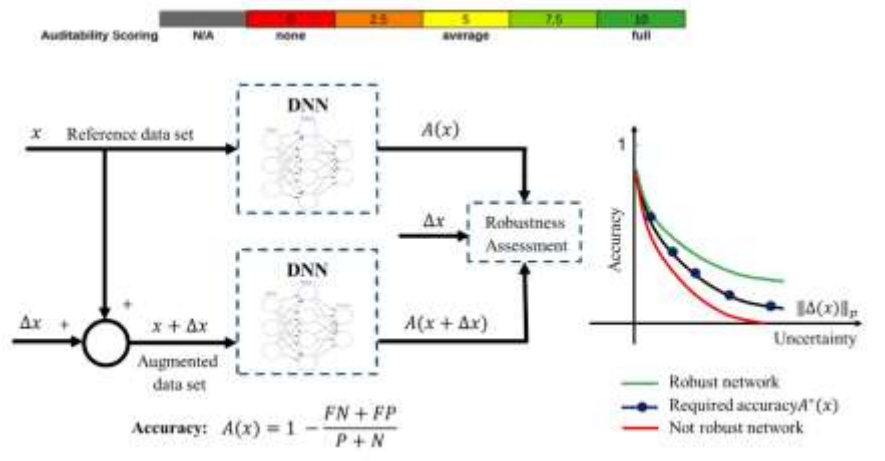
Christian Berghoff<sup>1</sup>, Jona Böddinghaus<sup>14</sup>, Vasilios Danos<sup>6</sup>, Gabrielle Davelaar<sup>13</sup>, Thomas Doms<sup>3</sup>, Heiko Ehrich<sup>6</sup>, Alexandru Forrai<sup>8</sup>, Radu Grosu<sup>9</sup>, Ronan Hamon<sup>10</sup>, Henrik Junklewitz<sup>10</sup>, Matthias Neu<sup>1</sup>, Simon Romanski<sup>11</sup>, Wojciech Samek<sup>7,15\*</sup>, Dirk Schlesinger<sup>4</sup>, Jan-Eve Stavesand<sup>12</sup>, Sebastian Steinbach<sup>2\*</sup>, Arndt von Twickel<sup>1\*</sup>, Robert Walter<sup>4</sup>, Johannes Weissenböck<sup>3</sup>, Markus Wenzel<sup>7</sup>, Thomas Wiegand<sup>7,15</sup> (Authors are listed in alphabetical order)

\*Contact:  
 Arndt von Twickel (arndt.twickel@bsi.bund.de),  
 Wojciech Samek (wojciech.samek@hhi.fraunhofer.de) and  
 Marc Fliehe (marc.fliehe@tuev-verband.de)

<sup>1</sup>Federal Office for Information Security Germany (BSI), <sup>2</sup>TÜV-Verband, <sup>3</sup>TÜV Austria, <sup>4</sup>TÜV AI Lab, <sup>5</sup>TÜV Süd, <sup>6</sup>TÜV Nord / TÜVIt, <sup>7</sup>Fraunhofer HHI, <sup>8</sup>Siemens Digital Industries Software, The Netherlands, <sup>9</sup>Technische Universität Wien, <sup>10</sup>European Commission, Joint Research Centre (JRC), <sup>11</sup>understand.ai GmbH, <sup>12</sup>dSPACE GmbH, <sup>13</sup>Microsoft, <sup>14</sup>Gradient Zero Deutschland GmbH, <sup>15</sup>TU Berlin

Lifecycle Phase / Aspect		Security	Safety	Performance	Robustness	Interpret-/ Explainability	Tracability	Risk Management
Embedding	organization	3	3	5	3	4	6	5
	use case specific requirements & risks	5	5	5	5	4	4	5
	Embodiment & situational awareness of AI module	5	5	5	5	6	3	5
AI module life cycle	planning phase	4	4	5	4	4	6	5
	data acquisition and QA phase	4	5	6	5	4	6	5
	training phase	5	5	5	5	6	6	5
	evaluation phase	5	5	5	5	6	6	5
	deployment and scaling phase	4	3	5	3	4	6	5
	operational (& maintenance) phase	5	3	5	3	4	6	6

Out of scope: user focused criteria (Safety, Bias, Data Privacy, Human oversight, ...)



## 8 вопросов от британского ICO, на которые нужно ответить перед использованием генеративного ИИ и больших языковых моделей

Британское Управление комиссара по информации (ICO) опубликовало 03.04.2023 года пресс-релиз, в котором указало восемь вопросов, которые разработчики и пользователи должны задавать при использовании генеративного искусственного интеллекта (ИИ) и больших языковых моделей (LLM), таких как ChatGPT. Организации, разрабатывающие или использующие генеративный ИИ, должны с самого начала учитывать свои обязательства по защите персональных данных, принимая в качестве обязательной практики подход "Защита данных по проекту и по умолчанию".

1. Какова законная основа для обработки персональных данных?
2. Является ли организация контролером, совместным контролером или обработчиком?
3. Подготовила ли организация оценку воздействия на защиту данных ("DPIA") перед обработкой персональных данных?
4. Как организация обеспечивает прозрачность?
5. Как организация будет снижать риски безопасности, включая риски инверсии модели и вывода о принадлежности, заражения данных и других форм атак со стороны злоумышленников?
6. Как организация будет ограничивать излишнюю обработку?
7. Как организация будет выполнять запросы на соблюдение прав субъектов данных?
8. Будет ли организация использовать генеративный ИИ для принятия исключительно автоматизированных решений?

## Руководство французского CNIL по созданию наборов данных для разработки систем ИИ

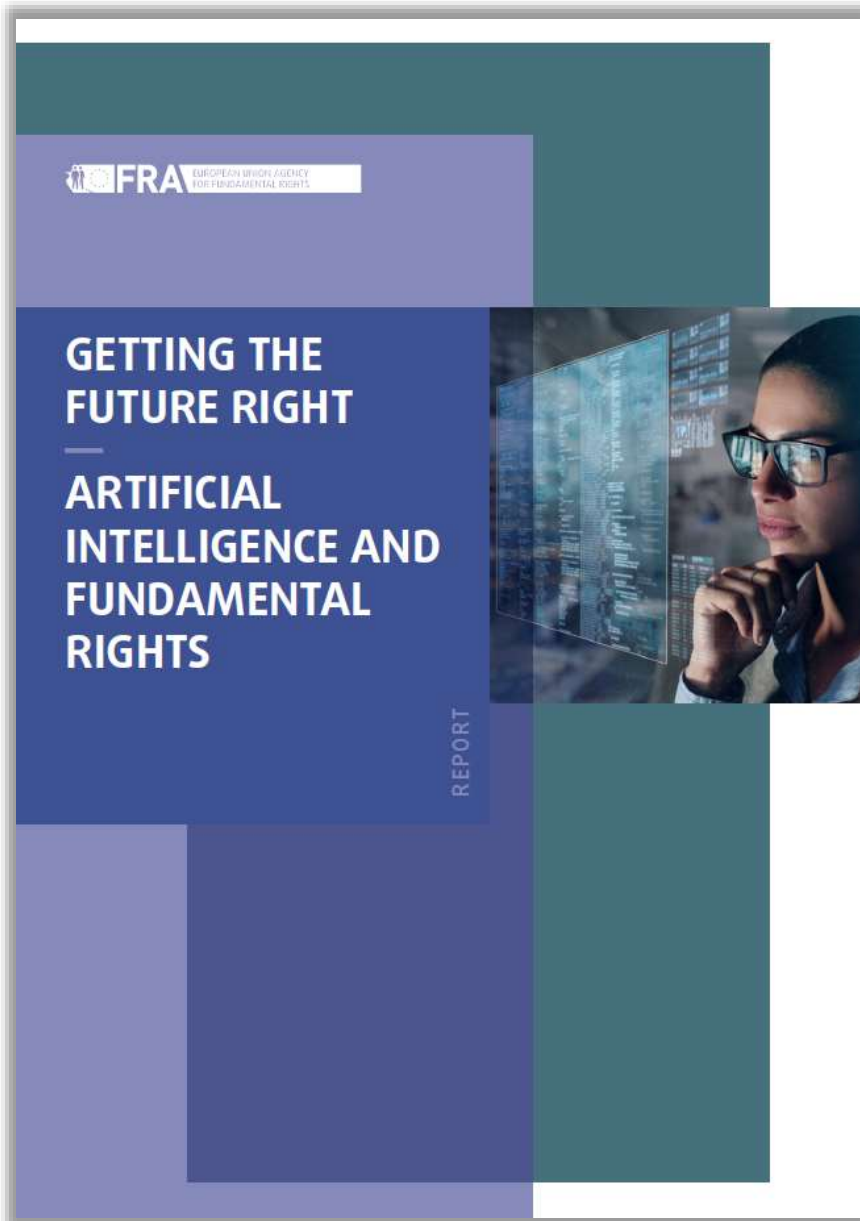


Французский орган по защите данных (CNIL) опубликовал 16.10.2023 руководство, состоящее из 9 документов, по созданию наборов данных для разработки систем искусственного интеллекта (ИИ) и начал публичные консультации по этому вопросу. Руководство даёт конкретные и практические ответы на юридические и технические вопросы, связанные с выполнением требований GDPR при применении ИИ.

◇ Так, в руководстве рассматриваются вопросы применения принципов ограничения цели обработки данных, минимизации и ограничения хранения данных, используемых для машинного обучения, а также разъясняются правила, применимые к научным исследованиям и повторному использованию данных.

◇ Что касается сферы применения документов, то она ограничивается этапом разработки ИИ, исключая, таким образом, этап внедрения и использования систем ИИ для обработки персональных данных.

## Исследование FRA по учету фундаментальных прав человека при разработке и использовании технологий ИИ



**Is it compliant?**

- Design and use must comply with relevant laws
- Any data processing must respect data protection laws
- Considers the wider impact on other rights

**Is it fair?**

- Does not discriminate on grounds such as ethnicity, age, disability, sex and sexual orientation
- Respects the rights of children, older people and people with disabilities

**Can it be challenged?**

- People are aware AI is being used
- People can complain about AI decisions
- Decisions based on the system can be explained

**Can it be checked?**

- Assess and regularly review use of AI for fundamental rights issues
- People applying AI can describe the system, its aim and data used

**Are external experts involved?**

- Consult with experts and stakeholders
- Expert oversight

# 447 Исследование действующих рекомендаций об этике ИИ

	The European Commission's Artificial Intelligence Act	Report on the Future of Artificial Intelligence	AI Ethics Guidelines	OECD Recommendation of the Council on Artificial Intelligence	The European Union of Artificial Intelligence	AI Ethics	The Address: AI Principles	AI Now 2017 Report	AI Now 2018 Report	AI Now 2019 Report	Principles for Automated Decision Making and a Social Impact Statement for Algorithms	Association for Computing Machinery's Department of Artificial Intelligence	OpenAI Charter	Ethically Aligned Design: A Vision for Meaningful Human-Computer Interaction and Intelligent Systems (First Edition)	Ethically Aligned Design: A Vision for Meaningful Human-Computer Interaction and Intelligent Systems (First Edition)	ITIL 4 Study Pack	Microsoft AI Principles	DeepMind Ethics & Society Principles	AI Ethics Principles at Google	Overarching Ethics for Artificial Intelligence	Partnership on AI	number of mentions
authors	(Pekala et al. 2018)	(Holdren et al. 2016)	Beijing Academy of Artificial Intelligence (2018)	Organisation for Economic Co-operation and Development (2019)	(Strudwig et al. 2018)	(Floridi et al. 2018)	(Future of Life Institute 2017)	(Crowford et al. 2016)	(Carpolo et al. 2017)	(Whittaker et al. 2018)	(Crowford et al. 2019)	(Dakopoulos et al.)	(Abney et al. 2018)	(OpenAI 2016)	(The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems 2016)	(The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems 2019)	(Information Technology Council 2017)	(Microsoft Corporation 2019)	(DeepMind)	(Google 2018)	(Culier et al. 2018)	(Partnership on AI 2018)
key issue	AI principles of the EU	AI principles of the US	AI principles of China	AI principles of the OECD	analysis of abuse scenarios of AI	meta-analysis about principles for the beneficial use of AI	large collection of different principles	statements on social implications of AI	statements on social implications of AI	statements on social implications of AI	statements on social implications of AI	statements on social implications of AI	principles of the FAT ML community	code of ethics released by the Universitat de Montreal	several short principles for the ethical use of AI	detailed description of ethical aspects in the context of AI	detailed description of ethical aspects in the context of AI	brief guidelines about basic ethical principles	short list of keywords for the ethical use of AI	several short principles for the ethical use of AI	IBM's short list of keywords for the ethical use of AI	principles of an association between several industry leaders
privacy protection																						18
fairness, non-discrimination, justice																						18
accountability																						17
transparency, openness																						16
security, cybersecurity																						16
common good, sustainability, wellbeing																						16
human oversight, control, auditing																						12
solidarity, inclusion, social cohesion																						11
explainability, interpretability																						10
science-policy link																						10
legislative framework, legal status of AI systems																						10
future of employment/worker rights																						9
responsible/international research funding																						8
public awareness, education about AI and its risks																						8
disinformation, military, AI arms race																						8
field-specific deliberations (health, military, mobility etc.)																						8
human autonomy																						7
diversity in the field of AI																						7
certification for AI products																						4
protection of whistleblowers																						3
cultural differences in the ethically aligned design of AI systems																						2
hidden costs (labeling, clickwork, content moderation, energy, resources)																						2
notes on technical implementations	yes, but very few	none	none	none	yes	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	
proportion of women among authors (f/m)	(8/10)	(2/3)	ns	ns	(5/21)	(5/8)	ns	(4/2)	(3/1)	(6/4)	(12/4)	(13/2)	(8/10)	ns	varies in each chapter	varies in each chapter	ns	ns	ns	ns	ns	(55/7)
length (number of words)	16546	22787	756	3249	34017	8609	646	13530	16273	23759	38970	1359	4754	441	40315	108032	2272	75	417	832	4488	1481
affiliation (government, industry, science)	government	government	science/gov./ind.	government	science	science	science	science	science	science	science	science	science	science	industry	industry	industry	industry	industry	industry	industry	industry
number of ethical aspects	9	12	13	12	8	14	12	13	9	12	13	5	11	4	14	18	9	6	6	6	6	8

## 448 NIST опубликовал Концепцию менеджмента рисков, связанных с ИИ



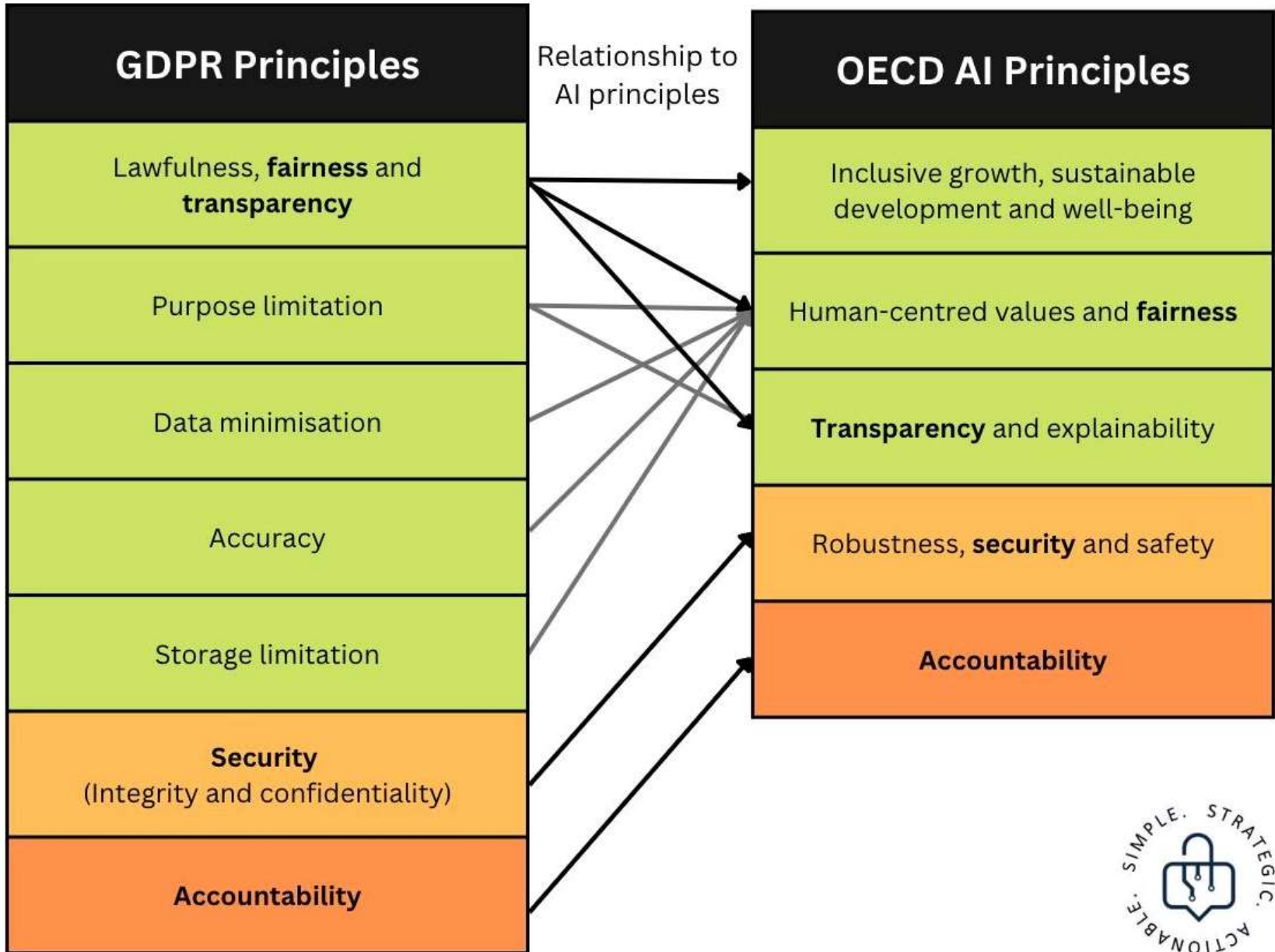
NIST разработал данную Концепцию в сотрудничестве с частным и государственным секторами, с целью лучшего управления рисками для отдельных лиц, организаций и общества, связанных с искусственным интеллектом (ИИ). «Концепция менеджмента рисков, связанных с искусственным интеллектом» предназначена для добровольного применения с целью повышения способности учитывать соображения, касающиеся надежности и доверия, при проектировании, разработке, использовании и оценка ИИ-продуктов, услуг и систем.

Представленная 26.01.2023 года Концепция была разработана в рамках основанного на консенсусе, открытого, прозрачного и коллективного процесса, который включал стадию запроса информации (Request for Information), подготовку нескольких предварительных версий для публичного обсуждения, проведение ряда семинаров и предоставление иных возможностей для подачи своих замечаний и предложений. Предполагается, что Концепция будет развивать, согласовываться и поддерживать усилия по управлению связанными с ИИ рисками, предпринимаемые другими сторонами.

NIST планирует сотрудничать с ИИ-сообществом с тем, чтобы периодически обновлять Концепцию, и готов в любое время рассматривать предложения по внесению в Концепцию дополнений и улучшений. Замечания и предложения, полученные до конца февраля 2023 года, будут включены в обновленную версию «Методических рекомендаций», которая выйдет в свет весной 2023 года.



449 Как соответствие GDPR поддерживает соблюдение принципов ИИ



## 450 Инструмент Давида Розенталя для оценки рисков при применении генеративного ИИ



Давид Розенталь опубликовал для публичного обсуждения новый инструмент — GAIRA — для оценки рисков применения генеративного ИИ в контексте конкретных проектов, на основе положений проекта Регламента ЕС по ИИ.

Подход к оценке похож на DPIA (оценку рисков для субъектов персональных данных), но покрывает также репутационные и финансовые риски, а также не строго юридические аспекты (ИИ-этика).

В инструмент (заполняемая эксель-таблица с формулами, см. приложение к этому посту) заранее включены 65 риск-сценариев, а также DPIA.

## 451 Досье CNIL по цифровой идентификации

Французский орган по защите данных ("CNIL") опубликовал 23.03.2023 тематическое досье по цифровой идентификации, в котором определяется понятие цифровой идентификации, описываются сценарии использования цифровой идентификации, и обязательства для организаций, использующих цифровую идентификацию.

Цифровая идентификация человека - это его различные нематериальные идентификационные данные, которые позволяют ему получить доступ к продуктам и услугам, с набором атрибутов, таких как псевдоним, фамилия, имя, возраст или место рождения, позволяющих связать эти данные с физическим лицом. Цифровая идентификация позволяет создать определенный уровень доверия для идентификации, которая позволяет отличить одно лицо от другого с помощью заданных идентификаторов, аутентификации, которая позволяет лицам доказать, что это одна из их личностей, и, наконец, подтверждения идентификации, которое позволяет продемонстрировать характеристики личности.

Также досье рекомендует использование:

- цифровых идентификаторов организациями, включая отказ от использования единого средства идентификации для всех онлайн-взаимодействий, что вызывает опасения по поводу отслеживания отдельных лиц;
- минимального объема личной информации, необходимой для требуемых целей, особенно для целей проверки возраста;
- децентрализованную архитектуру серверов идентификации для избегания возможного систематического мониторинга;
- прикладного интерфейса программирования (API) для обеспечения доступа пользователей только к тем данным, которые им необходимы;
- физических альтернатив цифровым идентификаторам, если они существуют.

В досье описываются риски уникальных и постоянных идентификаторов, состоящих из потенциально шести атрибутов личности (фамилия, имя, дата рождения, место рождения и т.д.), а также возможности постоянного профилирования, взаимосвязи файлов и систематического мониторинга. Высокий риск для субъектов данных связан с компрометацией биометрических данных, поскольку это может привести к сложному процессу получения нового идентификатора.



Законопроект предусматривает запрет использования технологий распознавания лиц для слежки за людьми, а также запрет применения алгоритмов, которые манипулируют поведением человека.

Как следует из справки, подготовленной **Центром регулирования искусственного интеллекта Сбербанка**, поправки в законодательство также предусматривают следующие меры:

- Члены ЕС должны будут утвердить органы для оценочного тестирования, сертификации и инспекции систем с ИИ.
- Компании, которые занимаются разработкой запрещенных услуг искусственного интеллекта, предоставляют неверную информацию или не сотрудничают с национальными властями, могут быть оштрафованы на сумму до 4% от годового дохода компании.
- Планируется создать «Европейский совет по искусственному интеллекту». Совету планируется поручить подготовку соответствующих рекомендаций и заключений для Европейской комиссии, касающихся перечня запрещенных методов использования ИИ, а также перечня «высокорисковых» систем ИИ.

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_1682](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682)

<https://techcrunch.com/2021/04/14/eu-plan-for-risk-based-ai-rules-to-set-fines-as-high-as-4-of-global-turnover-per-leaked-draft/>

## EDPB и EDPS призвали запретить применение искусственного интеллекта для распознавания лиц

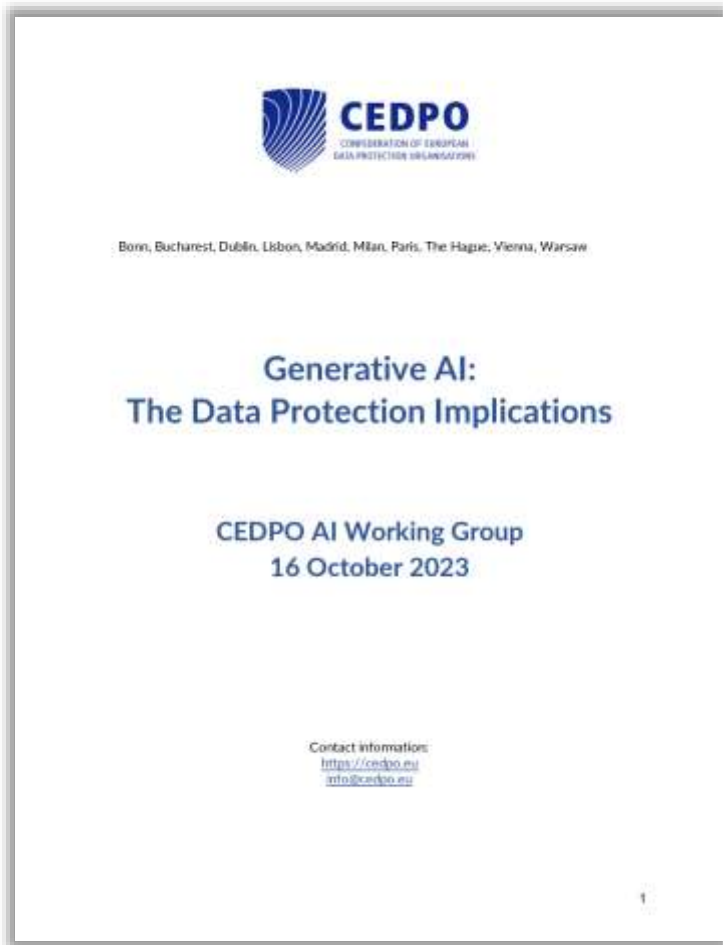


Два ведомства Евросоюза 21.06.2021 призвали полностью запретить применение искусственного интеллекта для распознавания лиц и других способов идентификации людей в общественных местах. Ранее Еврокомиссия предложила жестко ограничить, но не запрещать полностью использование ИИ в этой области.

"Если мы хотим сохранить наши свободы и создать ориентированное на человека законодательство об ИИ, то начать следует с общего запрета на системы распознавания лиц в общественных местах", - сказано в совместном заявлении глав Европейского совета по защите данных (The European Data Protection Board, EDPB) и Европейского надзорного органа по защите данных (European Data Protection Supervisor, EDPS) Андреа Елинек и Войцеха Вевэровского.

Они призывают запретить в общественных местах программы идентификации людей и по лицу, и по походке, по голосу, отпечаткам пальцев, ДНК и прочим биометрическим и поведенческим признакам.

Кроме того, главы EDPB и EDPS считают, что ЕС должен запретить и системы ИИ, которые классифицируют людей по этническому происхождению, полу, политическим взглядам или сексуальной ориентации. Применение систем, распознающих эмоции человека, они предлагают разрешить только в очень ограниченном наборе случаев - например, в медицине.

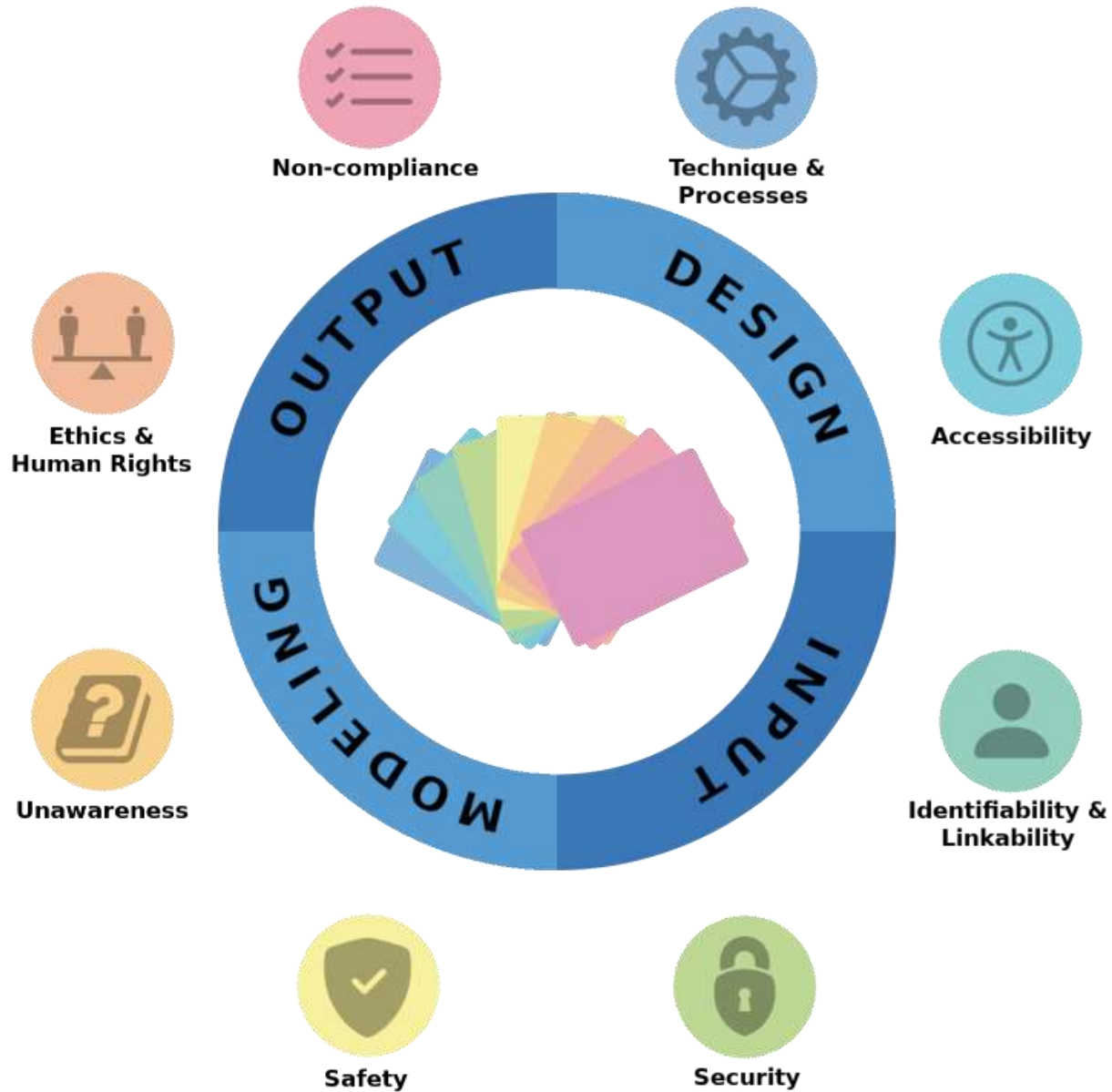


Конфедерация европейских организаций по защите данных (CEDPO) 26.10.2023 опубликовала документ, который содержит рекомендации по различным последствиям использования генеративных моделей искусственного интеллекта (ИИ) и методам, которые могут применять как создатели, так и конечные пользователи таких моделей для обеспечения соблюдения прав на защиту данных. В частности, среди прочих ключевых вопросов в документе рассматриваются:

- ◇ риски совместного использования данных;
- точность персональных данных;
- ◇ реализация принципа проектируемой защиты персональных данных;
- ◇ выбор законной основы для обучения генеративных систем искусственного интеллекта;
- ◇ оптимизация организационных структур;
- ◇ реализация прав субъектов данных в контексте ИИ.

CEDPO также дает рекомендации для создателей и конечных пользователей новых инструментов генеративного ИИ, чтобы обеспечить ограничение негативных последствий. Эти рекомендации включают, в частности, использование технологий, повышающих уровень конфиденциальности (PET), таких как использование синтетических наборов данных для обучения моделей ИИ, строгий внутренний контроль и аудит доступа к данным, а также использование оценок воздействия на защиту данных (DPIA).

455 Открытая библиотека угроз, связанных с использованием ИИ/МО



## 456 Google Cloud Vision запретили определять пол людей на фото

**Google AI will no longer use gender labels like 'woman' or 'man' on images of people to avoid bias**

Shara Ghosh | Published: 07/23/2020, 10:52 AM

Google CEO Sundar Pichai. Getty

- A Google AI tool that can recognize objects in pictures will no longer attach gender labels like "woman" or "man" to images of people.
- Google's Cloud Vision API is used by developers to analyze what's in an image, identifying anything from brand logos to faces to landmarks.
- Google emailed Cloud Vision API customers on Thursday morning stating that it won't use labels that pertain to gender because you can't deduce someone's gender by their appearance alone.
- An expert in AI bias told Business Insider that the change was a big positive.
- Visit Business Insider's homepage for more stories.

A Google AI tool that can recognize and label what's in an image will no longer attach gender tags like "woman" or "man" to photos of people.

**FIND A JOB**

Tech Jobs	C-Level Jobs
Media Jobs	Design Jobs
Finance Jobs	Sales Jobs

See All Jobs »

**POPULAR FROM #1 PRIME**

Here are the 11 companies that experts think Microsoft could try to acquire in 2020, including Salesforce, Twilio, and Workday

Этические правила человеческого общества повлияли и на искусственный интеллект. Алгоритмам Google запретили определять пол людей на фото из-за риска оскорбить трансгендеров.

Речь идёт о сервисе Google Cloud Vision API, который, помимо всего прочего, позволяет разработчикам ставить метки на фотографии, идентифицируя изображённые на них объекты. Теперь же алгоритмы не смогут выводить надписи «мужчина» или «женщина» на снимках.

В Google объяснили, что для изменений есть две причины. Во-первых, искусственный интеллект не всегда способен точно определить пол человека на основе его внешности. Во-вторых, такие метки могут дискриминировать отдельные категории людей, например, трансгендеров.

В итоге вместо меток о гендерной принадлежности алгоритм будет использовать надпись «человек».



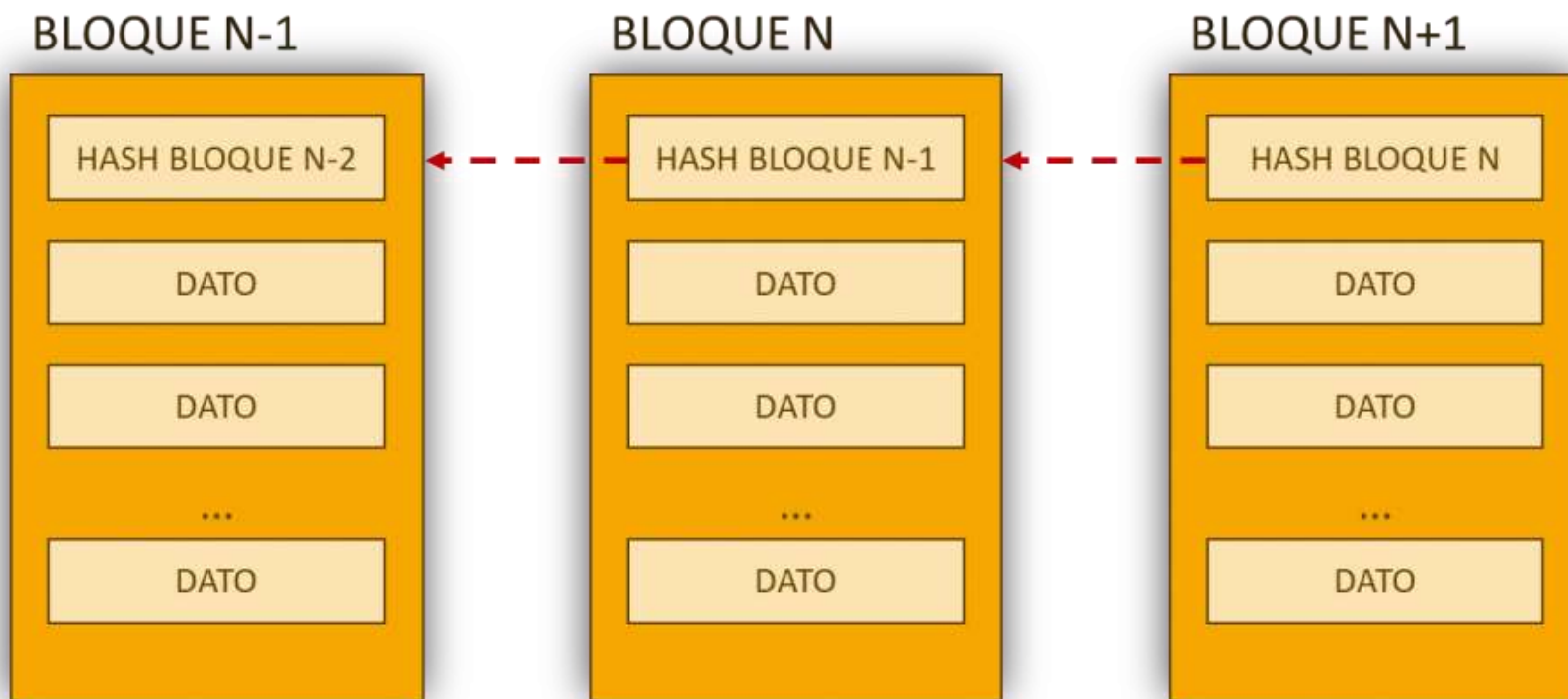


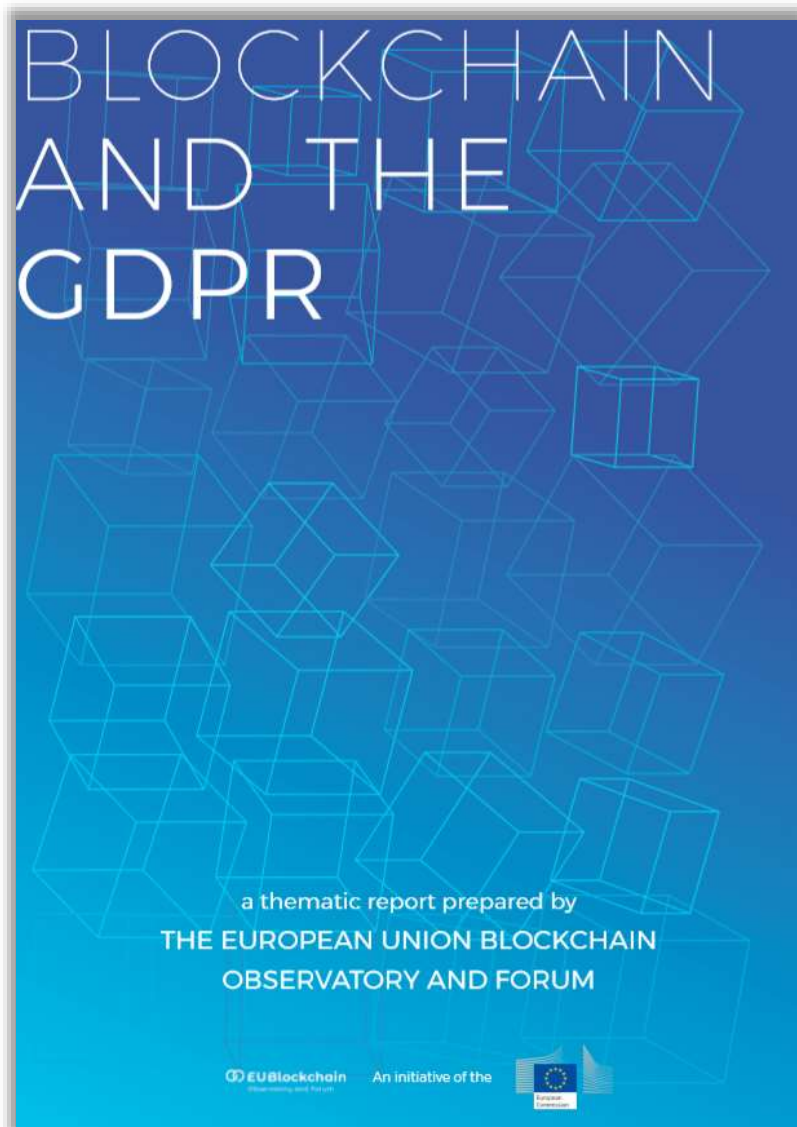
## Commission nationale de l'informatique et des libertés

Французский надзорный орган CNIL опубликовал отчет о специфике и особенностях использования технологии блокчейн в контексте обработки персональных данных и соблюдения требований GDPR.

## Руководство AEPD по смарт-контрактам в блокчейне и обработке персональных данных

Смарт-контракт — это программа, т. е. алгоритм, хранящийся в узлах блокчейна, который выполняет автоматизированные решения, например, финансового характера и управляет данными, связанными с цифровой идентификацией физического лица.





## Contents

4	<b>Executive summary</b>	
7	<b>Introduction</b>	
10	<b>Evolution from above: Introduction to the GDPR</b>	
	Personal data, the heart of the GDPR	10
	GDPR roles	11
	Principles, rights and obligations	12
14	<b>Revolution from below: Blockchain and the tools of decentralisation</b>	
	The decentralized database model	14
	Public blockchains and permissioned blockchains	14
	Is there a GDPR-compliant blockchain?	16
17	<b>Tensions between the GDPR and blockchain</b>	
	Accountability and roles: who is the controller?	17
	How should personal data be anonymised?	19
	Blockchains and the GDPR's rights and obligations	24
28	<b>Opposites attract: Resolving the tensions between blockchain and the GDPR</b>	
32	<b>Appendix</b>	
	Blockchain terminology	32
	Infographic	35

3

**EUBlockchain**  
Observatory and Forum

# Автоматизация Privacy и Data Protection



## 461 Website Evidence Collector от EDPS



### European Data Protection Supervisor

Бесплатное ПО для автоматизации проверки веб-сайтов, которое собирает информацию об обработке персональных данных, таких как файлы cookie или передачу данных третьим сторонам при посещении сайта. Собранные сведения, структурированные в машиночитаемом формате, позволяют администраторам веб-сайтов, DPO и конечным пользователям лучше понять, какая информация передается и хранится во время посещения веб-сайта.

#### Run Website Evidence Collection

```
links:
  count: 8
  entries:
    - edps.europa.eu
    - twitter.com
    - www.linkedin.com
    - www.youtube.com
    - www.europarl.europa.eu
    - forumti.pl
    - fra.europa.eu
    - edpb.europa.eu

user@linux :~$
```

# Онлайн сервис предоставления согласий на обработку данных от эстонского Riigi Infosüsteemi Ameti

REPUBLIC OF ESTONIA  
INFORMATION SYSTEM AUTHORITY

State information system Cyber Security EU Structural Funds Information System Authority Contacts

Home > State information system > Consent service

## Consent service

The consent service is an e-service developed by the Information System Authority which allows a person to give permission to the state to share their personal data with a certain service provider.

With the consent service, you can allow the transfer of your personal data to companies that offer innovative and personalised services based on personal data. Consents can only be given for the transfer of the data set required for a specific service. After consent has been given, the data held by the state is transferred to the private company that obtained the consent.

By using the consent service, you can decide on the processing of your personal data by choosing third parties who can access your data. The use of the consent service and the giving of consents is always voluntary. Consents can be revoked at any time.

**The consent service allows:**

- to give, review, and revoke consents;
- the data recipient to review the consents given to them for the release of data;
- the database to check whether consent has been given to the data recipient when issuing personal data.

The consent service has several good features for its users:

- convenient** – consent is always given in one trusted environment, regardless of the service provider;
- transparent** – consents and their usage history are available and managed in one place;
- safe** – consents are stored in a national database with a high level of security.

- Consent service documentation on GitHub »  
Open source will be added soon
- API on the X-tee »  
Consent service API
- Introduction to the consent service (1.13 MB, PDF)  
November 2021 (in Estonian)

The consent service is developed and managed by the Information System Authority.

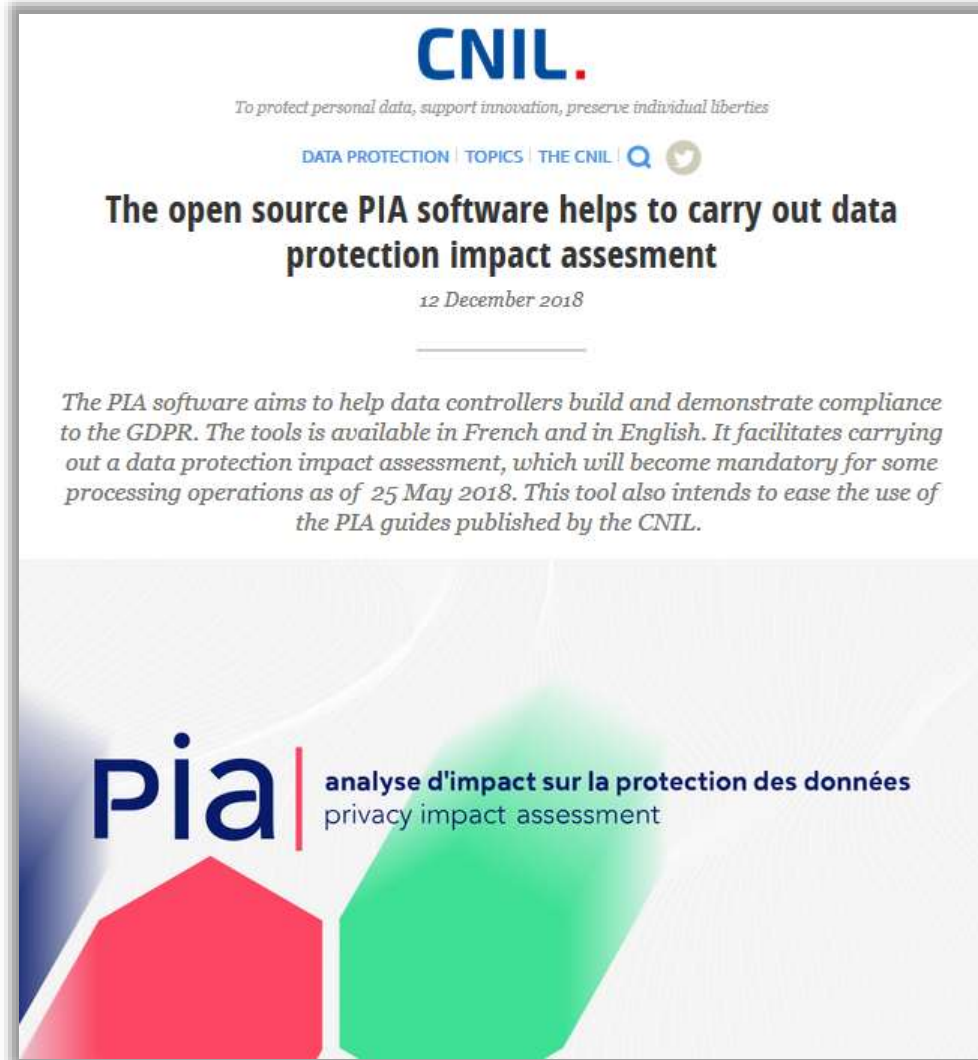
The development of the consent service started in **July 2020**. The first pilot project started in **December 2021**.

Contact: [help@\[ria.ee\]](mailto:help@[ria.ee])

<https://www.ria.ee/en/state-information-system/consent-service.html>

<https://www.dataguidance.com/opinion/estonia-personal-data-processing-consent-service>

## 463 Обзор CNIL по открытому ПО для осуществления DPIA



### Commission nationale de l'informatique et des libertés

Французский надзорный орган CNIL опубликовал обзор открытого программного обеспечения, облегчающего проведение data protection impact assesment (DPIA) согласно статье 35 GDPR.



**Privacy Program Management** – solutions designed specifically for the privacy office.

**Assessment managers** tend to automate different functions of a privacy program, such as operationalizing privacy impact assessments, locating risk gaps, demonstrating compliance and helping privacy officers scale complex tasks requiring spreadsheets, data entry and reporting.

**Consent managers** help organizations collect, track, demonstrate and manage users' consent.

**Data mapping** solutions can come in manual or automated form and help organizations determine data flows throughout the enterprise.

**Data subject request** solutions help organizations facilitate inquiries made by individuals who wish to exercise their data rights. These can include requests involving the right to access, rectification, portability and erasure.

**Incident response** solutions help companies respond to a data breach incident by providing information to relevant stakeholders of what was compromised and what notification obligations must be met.

**Privacy information managers** provide organizations with extensive and often automated information on the latest privacy laws around the world.

**Website scanning** is a service that primarily checks a client's website to determine what cookies, beacons and other trackers are embedded to help ensure compliance with various cookie laws and other regulations.

**Enterprise Privacy Management** – solutions designed to service the needs of the privacy office alongside the overall business needs of an organization.

**Activity monitoring** helps organizations determine who has access to personal data and when it is being accessed or processed. These solutions often come with controls to help manage activity.

**Data discovery** tends to be an automated technology that helps organizations determine and classify what kind of personal data they possess to help manage privacy risk and compliance.

**Deidentification/Pseudonymity** solutions help data scientists, researchers and other stakeholders derive value from datasets without compromising the privacy of the data subjects in a given dataset.

**Enterprise communications** are solutions that help organizations communicate internally in a secure way to avoid embarrassing or dangerous leaks of employee communications.





# CATALOG

## European Data Protection Technology Solutions

1<sup>st</sup> release

22 June 2023

### CATALOG. European Data Protection Technology Solutions

#### Catalog Table of Contents

	Page
Catalog Project Introduction	4
Legal Disclaimer	6
ABC Index	8
Country Index	9
Classification	10
Solutions:	
Bizoscore by Wandsoft Ltd	17
Piwik PRO	19
Signatu	21
Sitefig	23
Sypher	25
BIZONEO by Wandsoft Ltd	27
DPOrganizer	29
Data Privacy Manager by Legit	31
ASTRAN	33
Data Collaboration Platform by Datavillage	35
Sharemind by Cybernetica	37
Cosmian	39
Zama	41
Gallio PRO by Trasee sp.z o.o.	43
ECOMPLY	45
Enactia GRC	47
PrivacyEngine	49
PrivIQ	51
TPOmap by the Privacy Office Luxembourg	53
Wired Relations	55
Truata products	57
PrivacyGO by Wrangu	59
Openli	61
Dropvault	63
LegalXtract	65
YOKdata by Support2U	67
filerskeepers	69
Docbyte	71



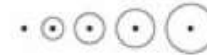
# Обзор Forrester по решениям для автоматизации управления комплаенсом в сфере защиты данных



## THE FORRESTER WAVE™ Privacy Management Software

Q4 2021

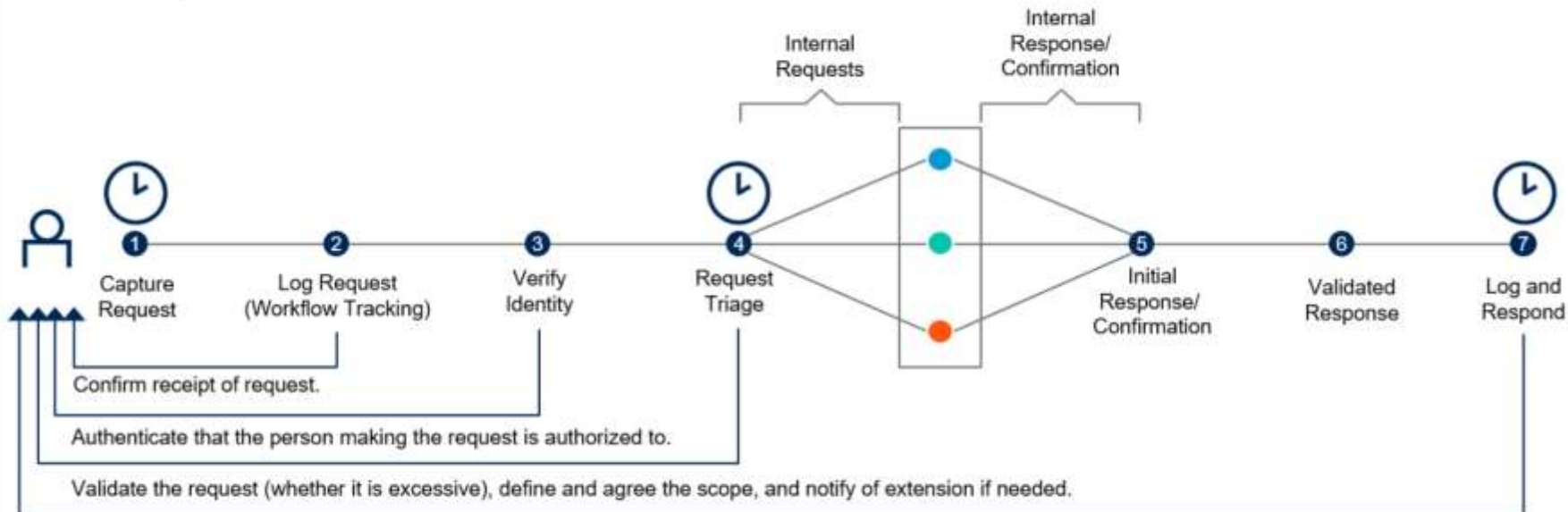
Market presence



## «Магический квадрат» от Gartner по сервисам управления рисками ИТ-поставщиков (август 2021)



## Subject Rights Fulfillment Workflow



Source: Gartner  
ID: 463762\_C

## Metrics for Efficiency and Investment Justification in SRR Handling



### Time

The time it takes to respond to a request.



### Cost

The financial cost of a request fulfillment.



### Scale

Capacity to respond within a certain time.

Source: Gartner  
ID: 463762\_C

## The Three Categories of Subject Rights Requests



**Informative**  
Access and Portability



**Corrective**  
Rectification and Erasure





**Restrictive**  
Limitations on Processing or Sale

Source: Gartner  
ID: 463762\_C



### Privacy Program Management

-  Readiness & Accountability Tool
-  Assessment Automation (PIA/DPIA)
-  Data Inventory & Mapping
-  Vendor Risk Management
-  Incident & Breach Management

### Small & Medium Enterprise

-  DPO Register for GDPR
-  SME Marketing Compliance

### Technology Integrations

-  Integrations Marketplace
-  OneTrust for ServiceNow

### Marketing & Web Compliance

-  Data Subject Rights Management
-  Website Compliance Scanning
-  Cookie Consent Management
-  Universal Consent Management
-  Enterprise Preference Center
-  IAB Publisher Consent
-  Mobile App Consent

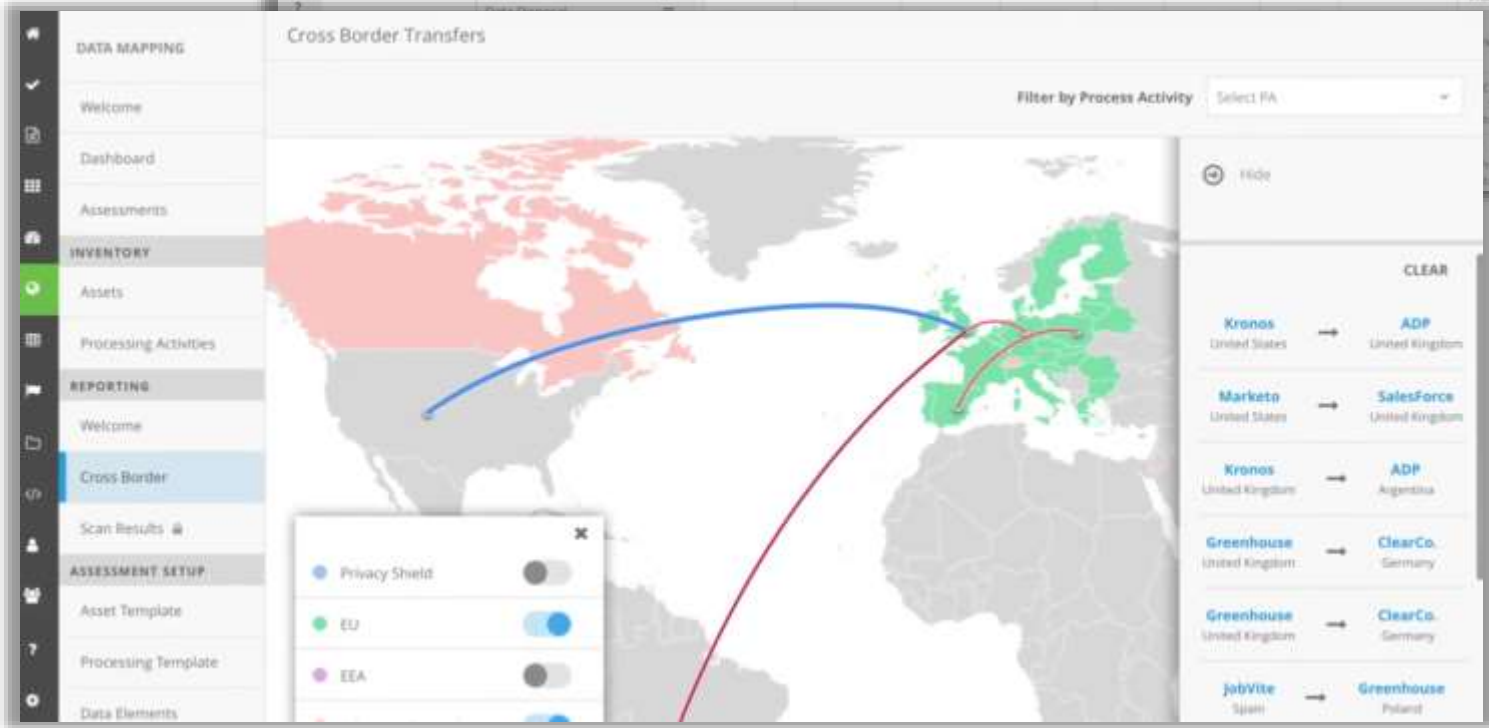
### GDPR & Global Privacy Solutions

-  GDPR Validation Program
-  GDPR Compliance
-  California Consumer Privacy Act
-  Brazil Law Compliance

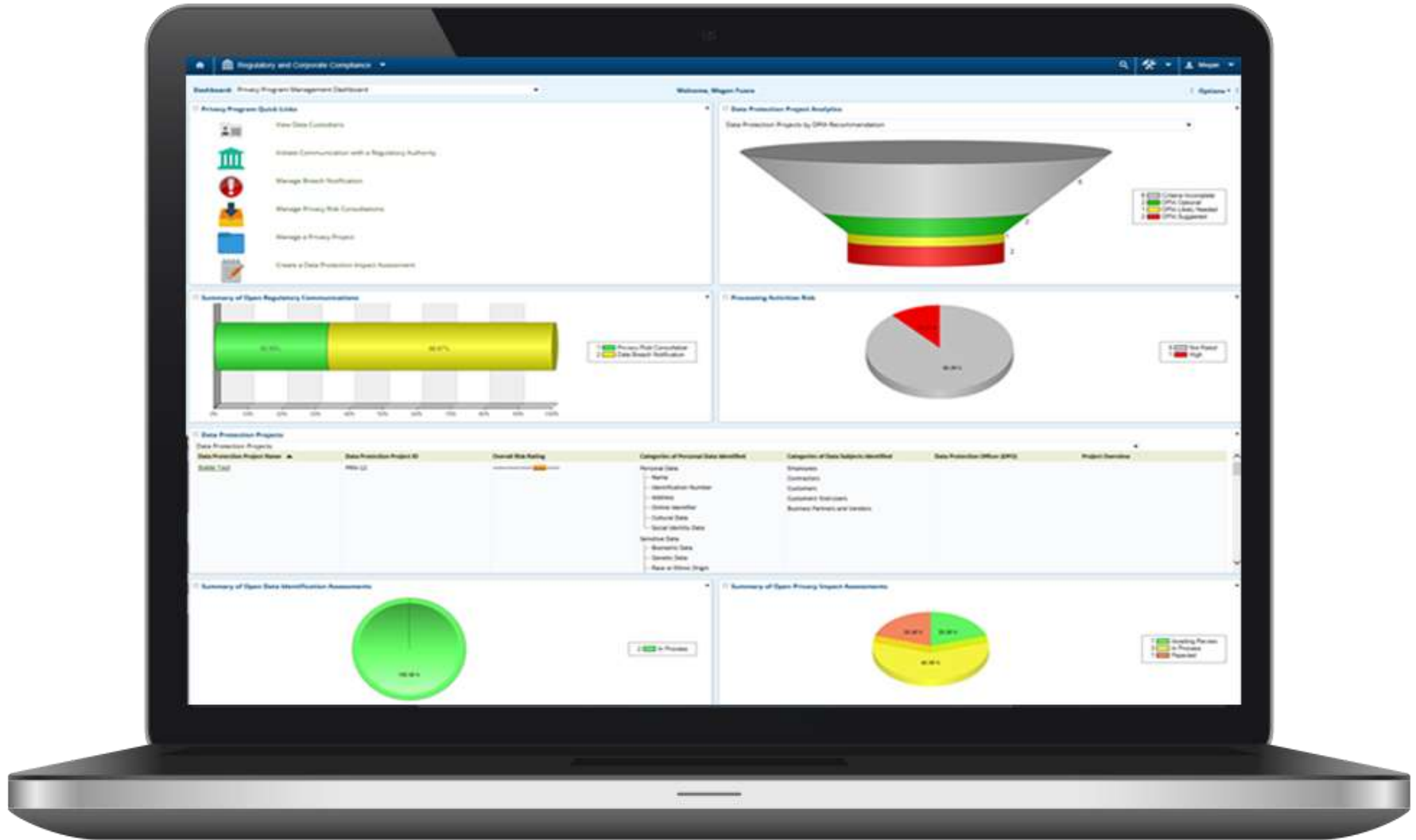
Reports / GDPR Article 30 Basic Requirements

Save Changes Save Report As Export Search Report

Processing Activity	Organization Group	Respondent	Application Name	In House vs 3rd Party	Application Host Country	Data Subjects	Data Elements	Data Purpose	Processor Name	Processor Address	Processor Phone Number
HR Recruiting	HR	Jennifer Lee	Greenhouse	3rd Party	United States	Prospective Hires	Drug Test Results, Criminal...More	Background Checks, Payroll...More	Skipped	Skipped	Skipped
Mobile Device Management	OneTrust	Jason Bourne	AirWatch	3rd Party	United States	Employees	Company / entity, job title...More	Corporate Data Access	Skipped	Skipped	Skipped
SaaS Products Procurement	OneTrust	Andrew Hnath	Salesforce	3rd Party	United States	Vendors	Credit checks, Tax identification...More	New Product Development	Skipped	Skipped	Skipped
HR Benefits Enrollment	HR	Jennifer Lee	Gusto	3rd Party	United States	Employees	Languages, Benefits and entitlements...More	Benefits	Skipped	Skipped	Skipped
SAP ERP Access	IT	Jason Bourne	SAP ECC6.0	3rd Party	Germany	Employees	Business unit / division...More	Customer Service, New Product...More	Skipped	Skipped	Skipped



# 471 RSA Archer Privacy Program Management







# 473 ARIS (Architecture of Integrated Information Systems)

ARIS Business Architect

File Edit View Insert Format Compare Arrange Hide/Show Evaluate Window Help

Balanced Scorecard

Modules Navigation Properties Symbols Fragments

Designer

Navigation Explorer tree Objects Model overview

Home Explorer Designer Matrices Administration Scripts Simulation

Properties

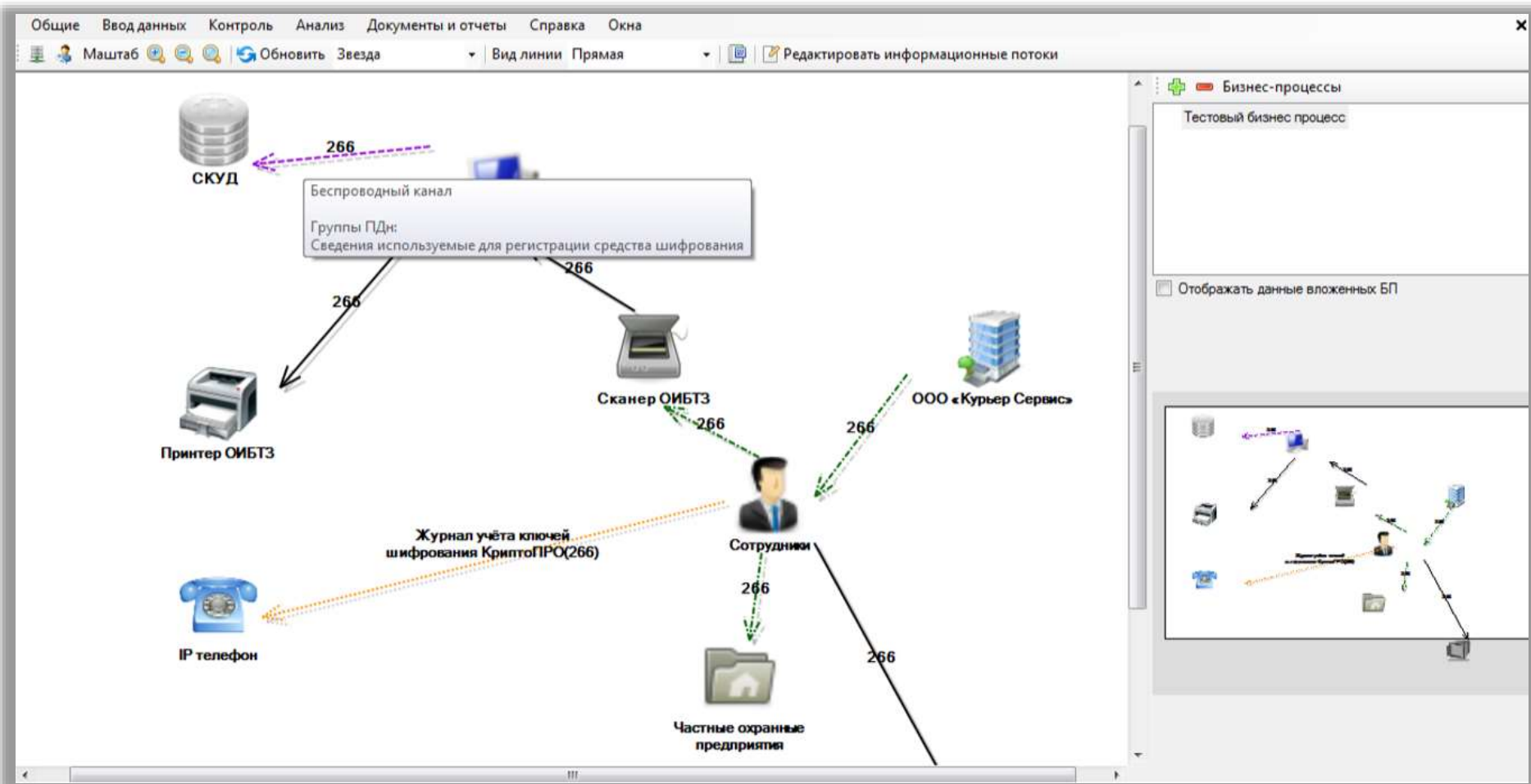
Attribut...	Balanced	Untitled
Name	Balanced Scorecard	
Identifier		
Descript...		
Synonyms		
Full name		
Remark/...		
Time of ...	2010-2-...	2010-2-...
Creator	system	system
Author	Методи	

More attributes...

Balanced Scorecard

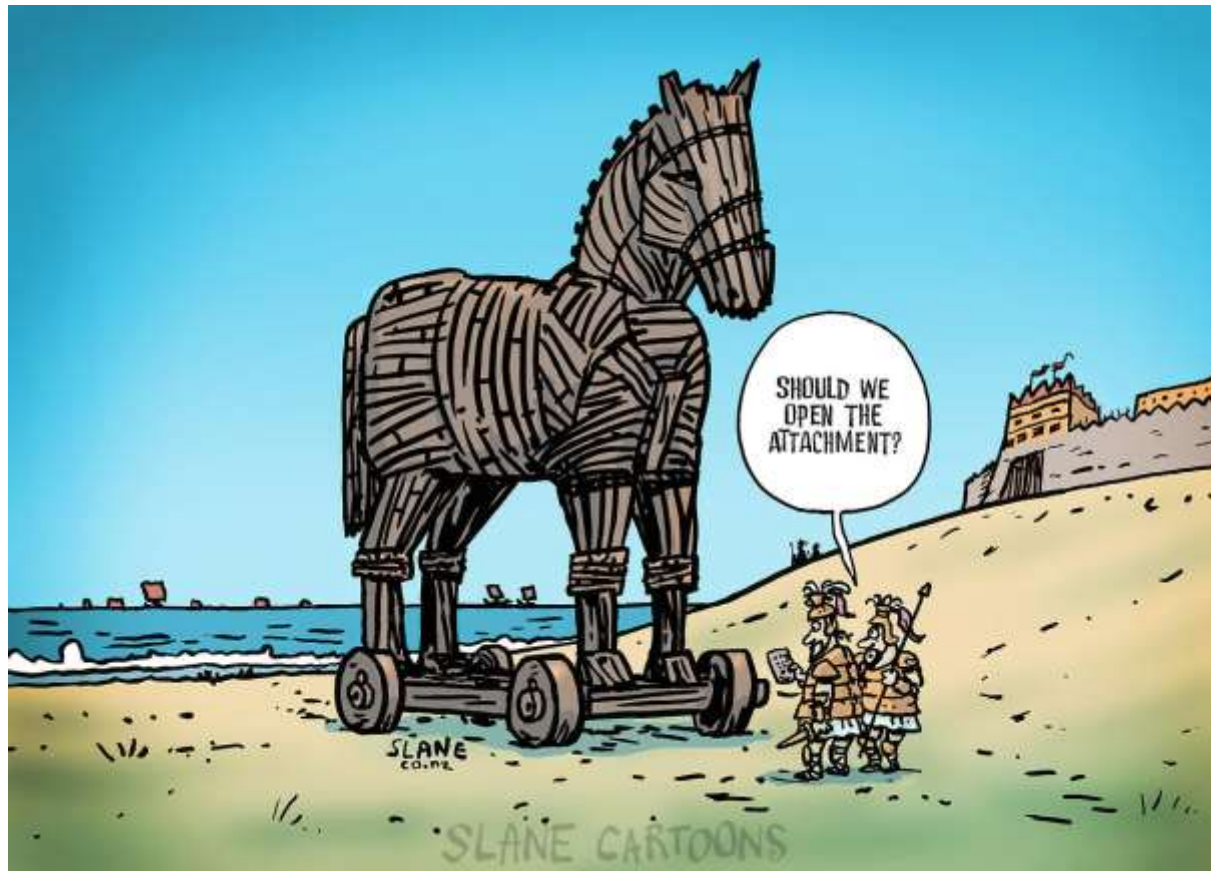
	Rel. per...	Cause-and-effect	Cause-and-effect
Strategy			
Perspective			
Perspective			
Perspective			
Perspective			

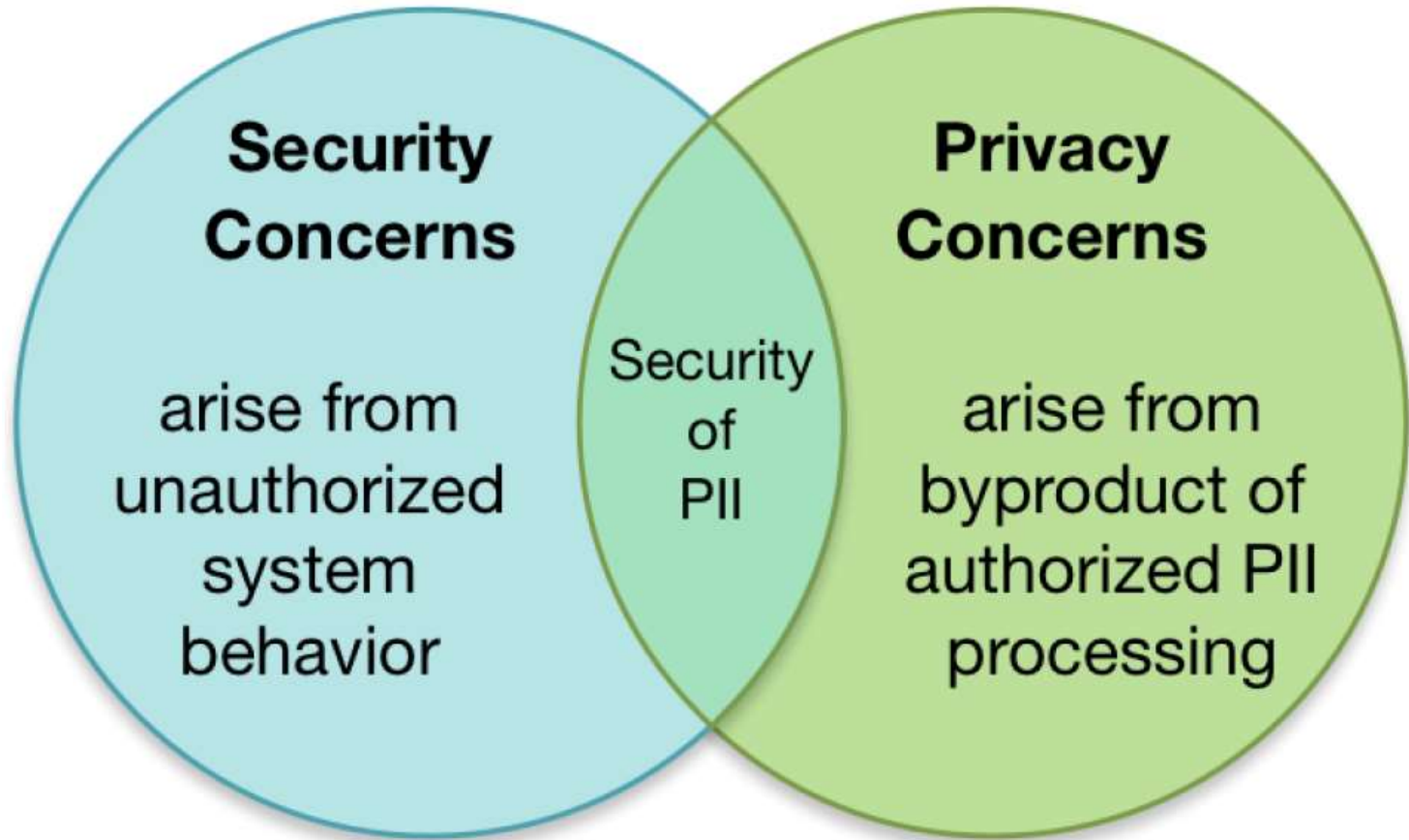
# Privacy-SPS (IRADD) - Пример интерфейса «Визуализация информационных потоков»



Privacy-SPS включено в Единый реестр российских программ для электронных вычислительных машин и баз данных - <https://reestr.minsvyaz.ru/reestr/73559/>

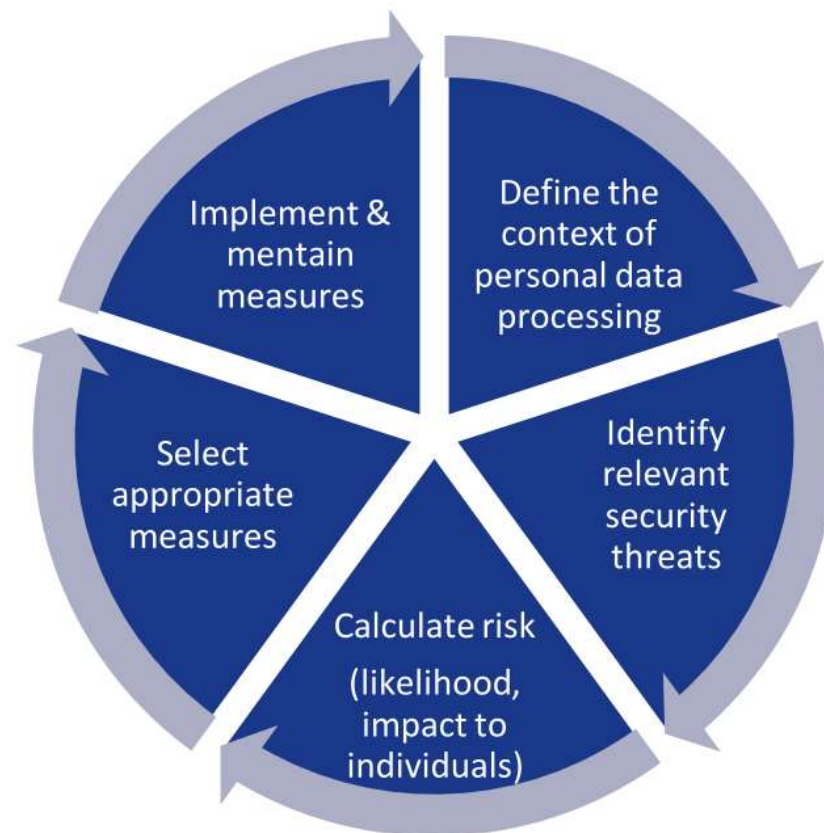
# Технические и организационные меры защиты персональных данных





## 477 Технические и организационные меры защиты в GDPR

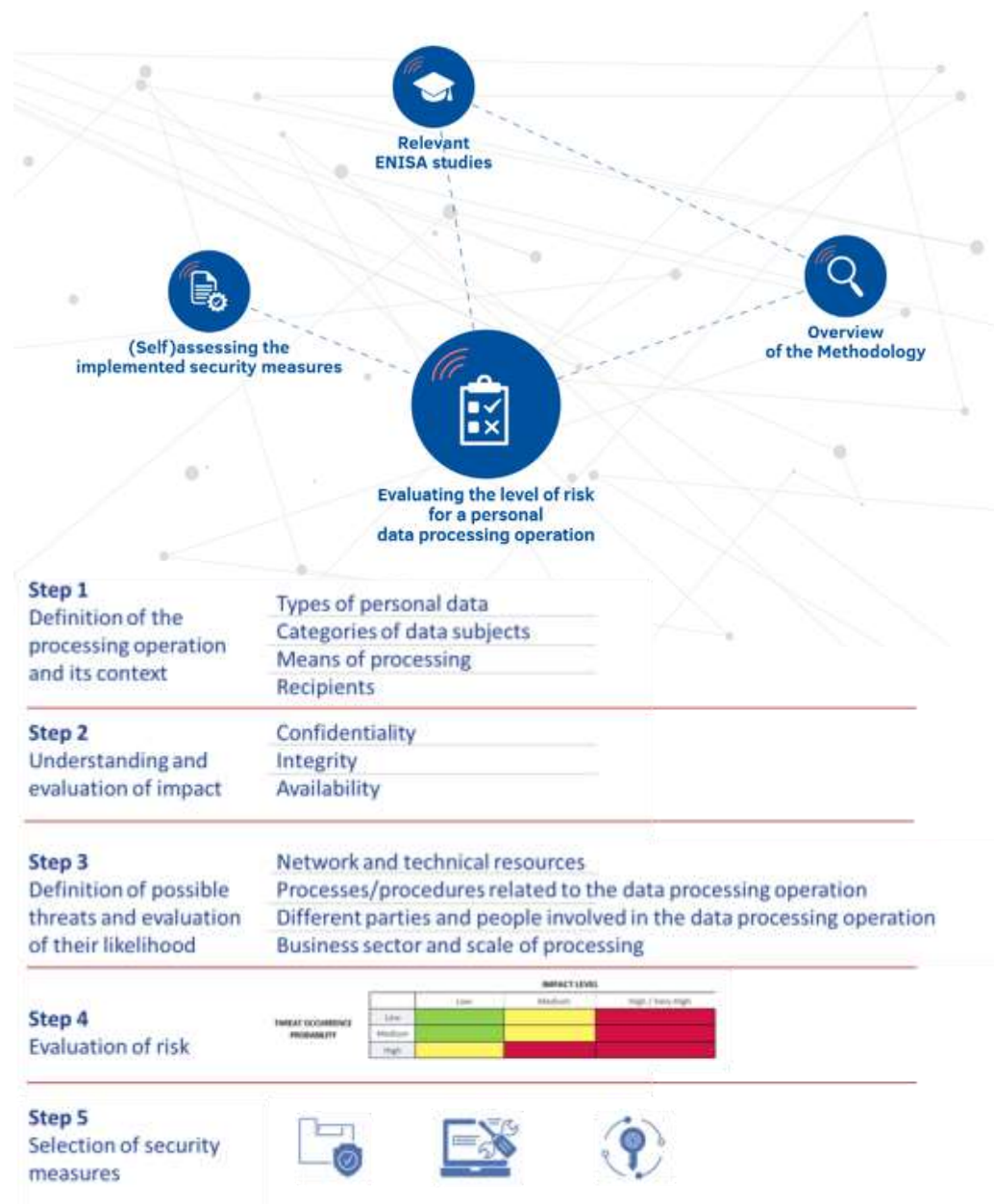
Reference	Properties	Category
Recital 29	Pseudonymisation, unlinkability, authorization	PP
Recital 66	Distribute data subject requests to processors	DSR
Recital 67	Restriction of processing	DSR
Recital 68	Data portability request	DSR
Recital 71	Accuracy of data	PP
Recital 78	Data minimization, pseudonymization, information	PP
Recital 81	Security	General
Recital 88	Protect data	General
Recital 156	Data minimization	PP
Art. 4 (5)	Pseudonymity	PP
Art. 5 (1) e	Non-identifiability	PP
Art. 5 (1) e	Storage limitation	PP
Art. 5 (1) f	Integrity and confidentiality	PP
Art. 17 (2)	Distribute data subject requests to processors	DSR
Art. 24 (1)	Demonstrate compliance	PP
Art. 24 (2)	Purpose limitation	PP
Art. 25 (1)	Pseudonymisation	PP
Art. 25 (2)	Data minimization	PP
Art. 28 (1)	meet the requirements of this regulation	General
Art. 28 (3) e	Distribute and execute data subject requests	DSR
Art. 28 (4)	meet the requirements of this regulation	General
Art. 32 (1) a	Pseudonymization	PP
Art. 32 (1) a	Encryption	PP
Art. 32 (1) b	Confidentiality, integrity, availability, resilience	PP
Art. 32 (1) c	access	PP
Art. 34 (3) a	render data unintelligible – (encryption, unlinkability)	PP
Art. 83 (2) d	Technical measures will be taken into account when determining fines	General



Security risk management for personal data



## Онлайн-платформа от ENISA по обеспечению безопасности персональных данных



<https://www.enisa.europa.eu/risk-level-tool/>

<https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform>



## Исследование по информационной безопасности в сфере электронных коммуникаций и онлайн-услуг от ENISA



В этом исследовании представлен обзор устоявшихся методов обеспечения информационной безопасности, которой призван помочь среднему и малому бизнесу составить представление о современном уровне развития технологий (State-of-the-Art) защиты информации по ряду направлений, представленных в практическом руководстве ENISA по защите данных.



		IMPACT LEVEL		
		Low	Medium	High / Very High
Threat Occurrence Probability	Low	Low Risk	Medium Risk	High Risk
	Medium	Low Risk	Medium Risk	High Risk
	High	Medium Risk	High Risk	High Risk

### Legend



Low Risk

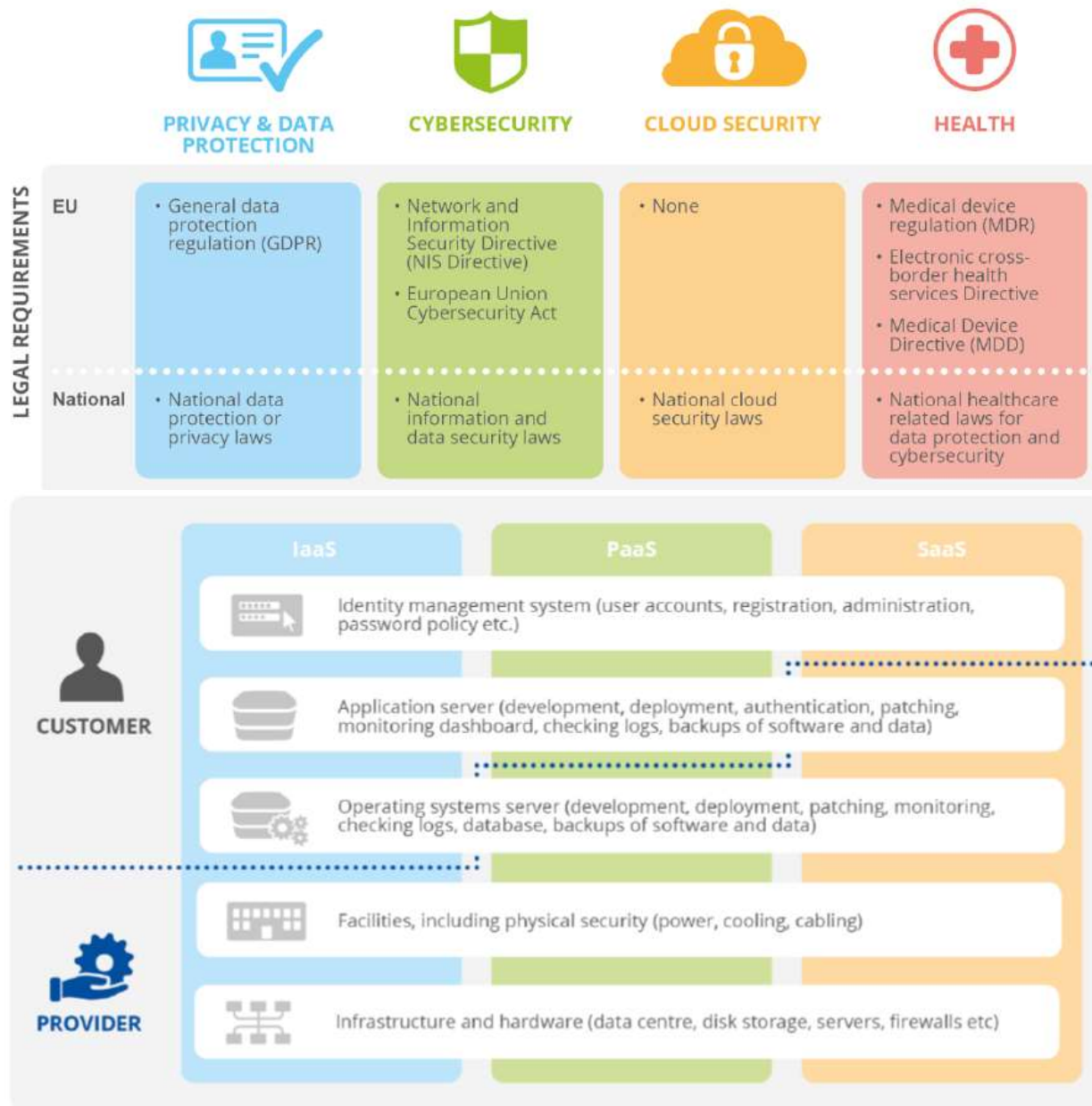


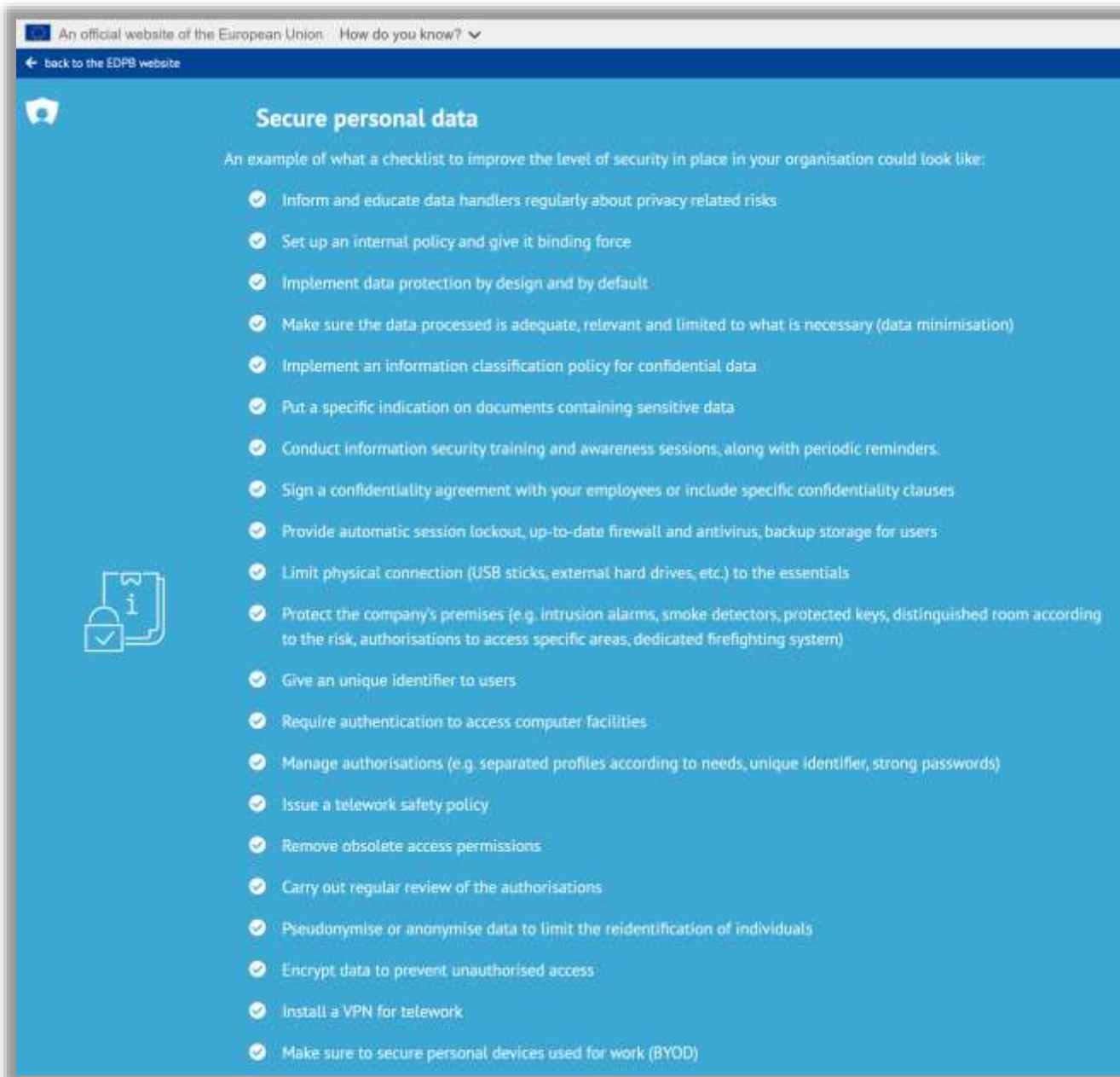
Medium Risk



High Risk

## Исследование по обеспечению ИБ облачных сервисов для здравоохранения от ENISA






An official website of the European Union How do you know? ▾

← back to the EDPB website

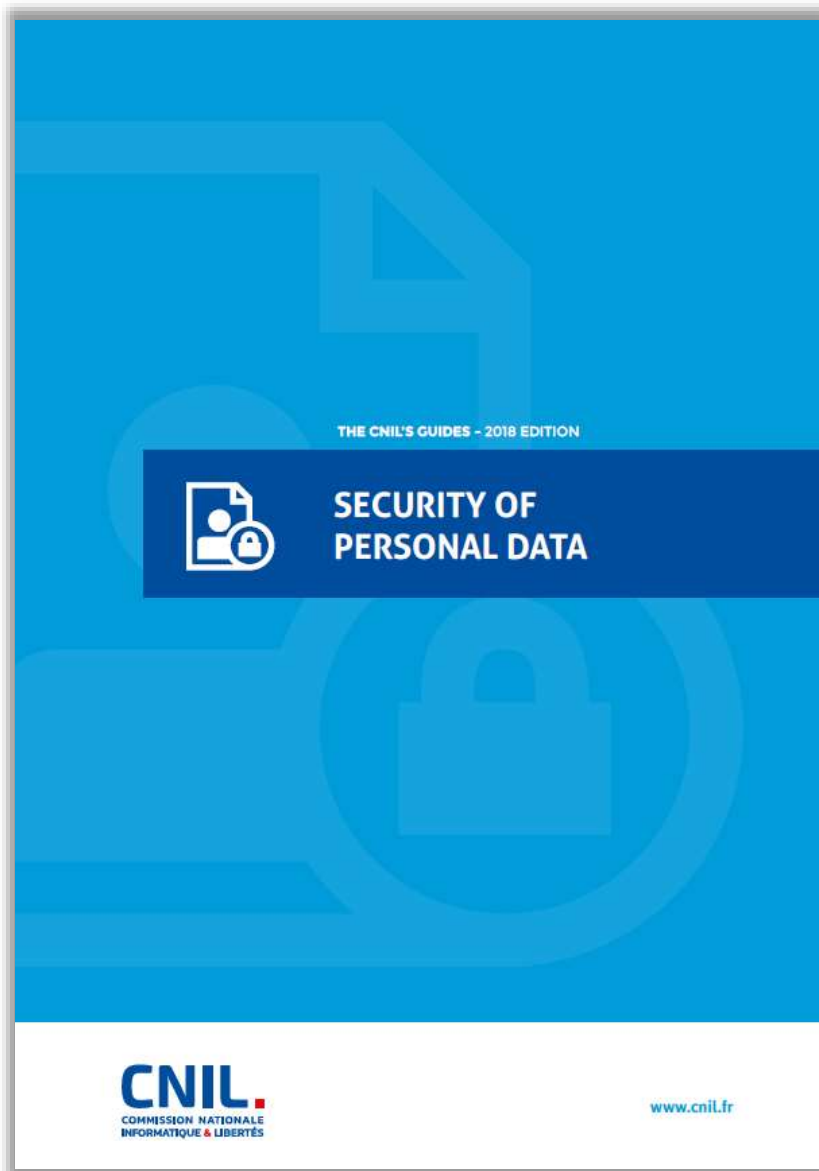
### Secure personal data

An example of what a checklist to improve the level of security in place in your organisation could look like:

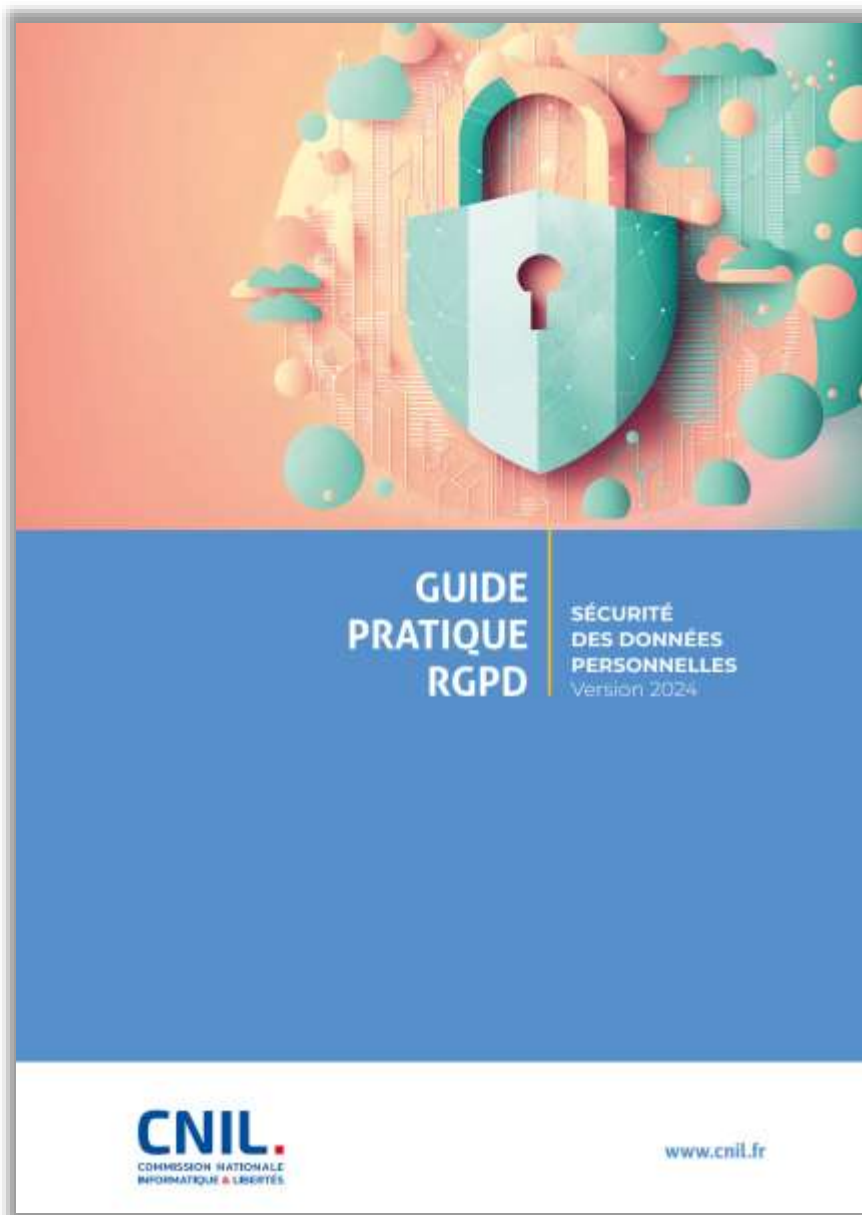
- ✓ Inform and educate data handlers regularly about privacy related risks
- ✓ Set up an internal policy and give it binding force
- ✓ Implement data protection by design and by default
- ✓ Make sure the data processed is adequate, relevant and limited to what is necessary (data minimisation)
- ✓ Implement an information classification policy for confidential data
- ✓ Put a specific indication on documents containing sensitive data
- ✓ Conduct information security training and awareness sessions, along with periodic reminders
- ✓ Sign a confidentiality agreement with your employees or include specific confidentiality clauses
- ✓ Provide automatic session lockout, up-to-date firewall and antivirus, backup storage for users
- ✓ Limit physical connection (USB sticks, external hard drives, etc.) to the essentials
- ✓ Protect the company's premises (e.g. intrusion alarms, smoke detectors, protected keys, distinguished room according to the risk, authorisations to access specific areas; dedicated firefighting system)
- ✓ Give an unique identifier to users
- ✓ Require authentication to access computer facilities
- ✓ Manage authorisations (e.g. separated profiles according to needs, unique identifier, strong passwords)
- ✓ Issue a telework safety policy
- ✓ Remove obsolete access permissions
- ✓ Carry out regular review of the authorisations
- ✓ Pseudonymise or anonymise data to limit the reidentification of individuals
- ✓ Encrypt data to prevent unauthorised access
- ✓ Install a VPN for telework
- ✓ Make sure to secure personal devices used for work (BYOD)



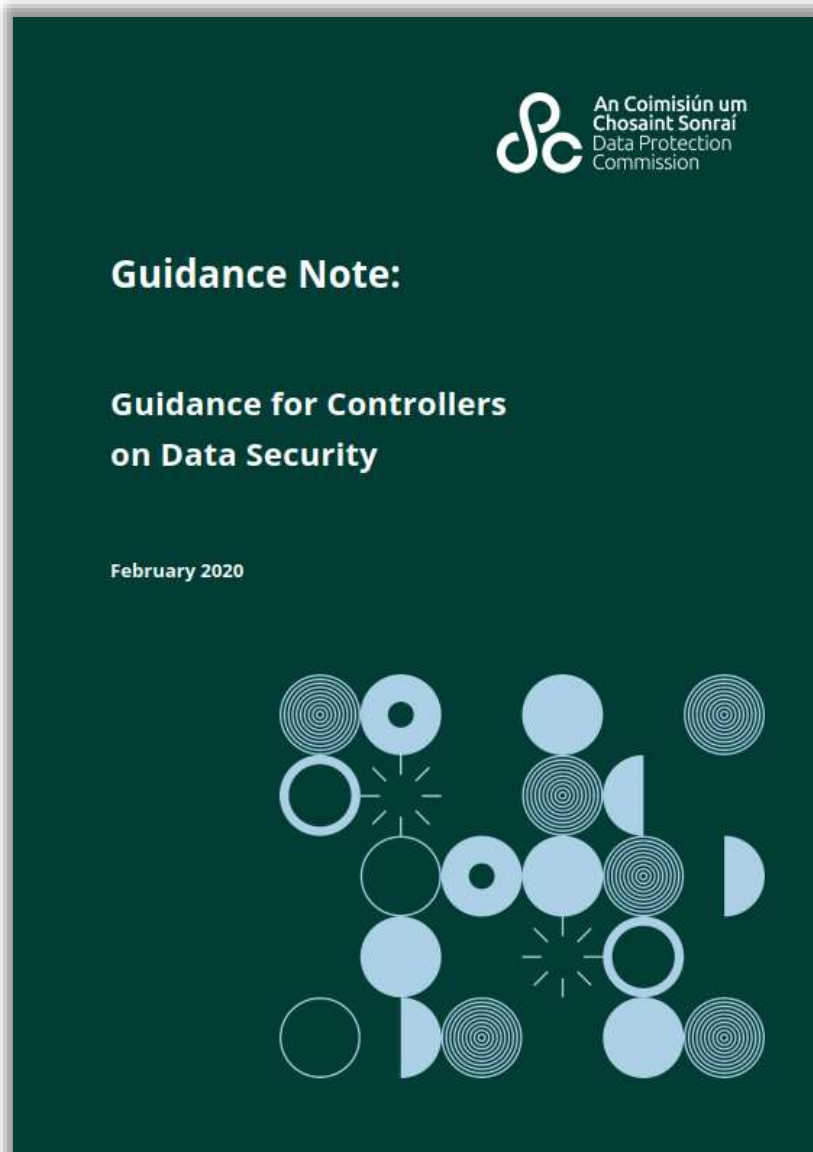
# Руководство CNIL от 2018 года по управлению рисками ИБ в рамках обеспечения защиты персональных данных



FACTSHEET	MEASURE
1 Raising user awareness	Inform and raise awareness among individuals handling data Write an IT charter and enforce its application
2 Authenticating	Define a unique identifier (login) for each user Adopt a user password policy conform to our recommendations Require each user to change his or her password whenever it has been resetted Limit the number of access attempts to an account
3 Access Management	Define authorisation profiles Remove obsolete access permissions Carry out an annual review of authorisations
4 Logging access and managing incidents	Implement a logging system Inform users of the implementation of the logging system Protect logging equipment and the information logged Organise the procedures for personal data breach notifications
5 Securing workstations	Organise an automatic session locking procedure Use regularly updated antivirus software Install firewall software Collect the user's consent before any intervention on his or her workstation
6 Securing mobile data processing	Organise encryption measures for mobile equipment Undertake regular data backups and synchronisations Require a confidential piece of information to unlock smartphones
7 Protecting the internal network	Limit the network traffic to the bare essentials Secure remote access to mobile computing devices via VPN Implement the WPA2 or WPA2-PSK protocol for Wi-Fi networks
8 Securing servers	Allow access to tools and administration interface only to qualified individuals Install critical updates without delay Ensure availability of data
9 Securing websites	Use the TLS protocol and check its implementation Check that no password or identifier are transferred via URLs Check that the user inputs correspond to what is expected Place a consent banner for cookies not required by the service
10 Ensuring continuity	Carry out regular backups Store the backup media in a secure place Organise security measures for the transport of backups Organise and regularly test the business continuity
11 Archiving securely	Implement specific access methods to archived data Destroy obsolete archives securely Record maintenance in a register
12 Supervising maintenance and data destruction	Have a responsible person from the organisation supervise work by third parties Delete the data from all hardware before it is discarded Add a specific clause in the contracts of subcontractors
13 Managing dataprocessors	Organise the restitution and destruction conditions of data Ensure the effectiveness of provided guarantees (security audits, visits, etc.) Encrypt data before sending it
14 Securing exchanges with other organisations	Ensure that it is the right recipient Send the secret information separately and via a different channel
15 Physical security	Restrict access to the premises via locked doors Install anti-intrusion alarms and check them periodically Offer parameters that respect the privacy of end users
16 Supervising software development	Avoid comment zones or supervise them strictly Carry out tests on fictional or anonymised data
17 Using cryptographic functions	Use recognised algorithms, software and libraries Keep the secret information and cryptographic keys in a secure way



AVANT-PROPOS	4
FICHE N° 1 <b>Piloter la sécurité des données</b>	5
<b>LES UTILISATEURS</b>	
FICHE N° 2 <b>Définir un cadre pour les utilisateurs</b>	9
FICHE N° 3 <b>Impliquer et former les utilisateurs</b>	11
FICHE N° 4 <b>Authentifier les utilisateurs</b>	13
FICHE N° 5 <b>Gérer les habilitations</b>	16
<b>MON INFORMATIQUE, MES ÉQUIPEMENTS</b>	
FICHE N° 6 <b>Sécuriser les postes de travail</b>	18
FICHE N° 7 <b>Sécuriser l'informatique mobile</b>	20
FICHE N° 8 <b>Protéger le réseau informatique</b>	22
FICHE N° 9 <b>Sécuriser les serveurs</b>	24
FICHE N° 10 <b>Sécuriser les sites web</b>	26
FICHE N° 11 <b>Encadrer les développements informatiques</b>	28
FICHE N° 12 <b>Protéger les locaux</b>	30
<b>MA MAÎTRISE DES DONNÉES</b>	
FICHE N° 13 <b>Sécuriser les échanges avec l'extérieur</b>	33
FICHE N° 14 <b>Gérer la sous-traitance</b>	35
FICHE N° 15 <b>Encadrer la maintenance et la fin de vie des matériels et logiciels</b>	37
<b>SE PRÉPARER À UN INCIDENT</b>	
FICHE N° 16 <b>Tracer les opérations</b>	40
FICHE N° 17 <b>Sauvegarder</b>	42
FICHE N° 18 <b>Prévoir la continuité et la reprise d'activité</b>	43
FICHE N° 19 <b>Gérer les incidents et les violations</b>	44
<b>FOCUS</b>	
FICHE N° 20 <b>Analyse de risques</b>	47
FICHE N° 21 <b>Chiffrement, hachage, signature</b>	50
FICHE N° 22 <b>Cloud : Informatique en nuage</b>	52
FICHE N° 23 <b>Applications mobiles : Conception et développement</b>	55
FICHE N° 24 <b>Intelligence artificielle : Conception et apprentissage</b>	57
FICHE N° 25 <b>API : Interfaces de programmation applicative</b>	59
<b>ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE MON ORGANISME</b>	61



Data Collection and Retention Policies	Wireless Networks.....
Access Controls.....	Portable Devices.....
Access Authentication.....	Logs and Audit Trails.....
Automatic Screen Savers.....	Back-Up Systems.....
Encryption .....	Incident Response Plans
Anti-Virus Software .....	Disposal of Equipment ...
Firewalls .....	Physical Security .....
Software Patching .....	The Human Factor.....
Remote Access.....	Certification.....



Organ po защите данных (Datatilsynet) 29.11.2023 опубликовал каталог технических и организационных мер, необходимых для обеспечения безопасности обработки данных в соответствии со статьями 5 и 32 GDPR.

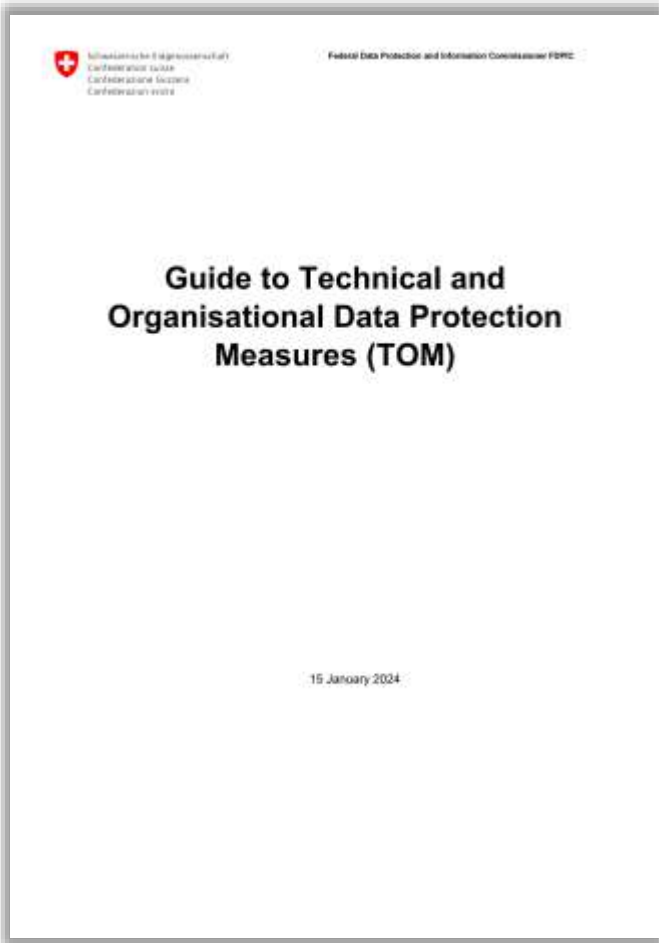
Технические меры:

- автоматическое шифрование;
- многофакторная аутентификация (MFA);
- автоматический контроль доступа;
- ведение журнала использования персональных данных пользователями;
- физический контроль доступа.

Организационные меры:

- минимизация привилегированных прав доступа;
- внедрение ролевых прав доступа;
- документирование разрешений на доступ к данным;
- установление процедур отзыва.

# 488 Рекомендации швейцарского FDPIС по обеспечению безопасности данных



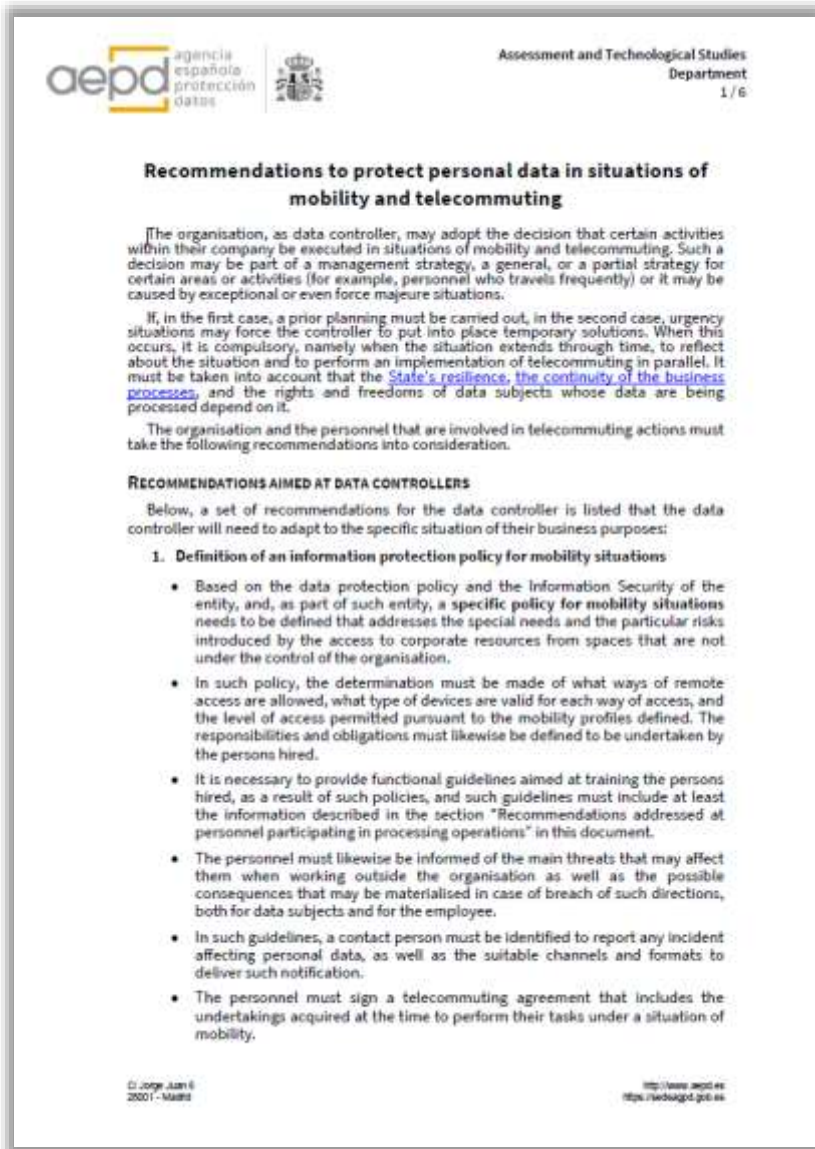
Standards					Measures on...	Laws / Regulations			Other
COBIT	BSI	CH-MS	ISO 27001	ISO 27701		FADP	DPO	GDPR	EDPB <sup>1</sup>
X	X	X	X		Data sharing and transfer (external)	X	X	X	
X	X	X	X		Processing (internal)	X	X	X	
X	X	X	X		Infrastructure	X	X	X	
				X	The data itself	X	X	X	X
					Personnel involved	X	X	X	X

Table 1: Steps to be taken during data processing, the laws that require them, and the standards that cover them.<sup>2</sup> For the sake of clarity, please note the distinction made in this guide between 'data protection' and 'data security' (see section 1.2 above).

	CH-MS [1]	CNIL [8]	ISO 27002 [9]
Configuring mobile devices	Sec. 1.6.9	Sheet 6	Sec 6.7
Elements of a defence in depth strategy	Sec. 1.6		
Equipment lifecycle management	Sec. 1.6.8	Sheet 13	Sec. 7.14
Workstation management		Sheet 5	Sec. 7.6 – 7.8
Risk management	Sec 1.6.3, 2.2.4-6		
Maintenance	Sec. 2.3.5		Sec. 7.13
Host security	Sec. 1.6.13		
Network security		Sheet 7, 8	Sec 8.20 - 8.22
Physical / equipment security	Sec. 1.6.7, 2.3.3	Sheet 16	Sec. 7.3 – 7.5



## Рекомендации AEPD по защите персональных данных в условиях мобильности и удаленного взаимодействия



В апреле 2020 испанский уполномоченный орган опубликовал рекомендации для контролеров и их персонала по защите персональных данных в условиях мобильности и удаленного взаимодействия. В частности, рекомендуется следующее:

- определение политики защиты информации для условий удаленного взаимодействия;
- выбор поставщиков решений и услуг, которые заслуживают доверия и предлагают гарантии;
- ограничение доступа к информации;
- правильная настройка оборудования и устройств, используемых для удаленного взаимодействия;
- мониторинг удаленного доступа к корпоративной вычислительной сети;
- рациональное управление защитой и безопасностью данных.

## 490 Руководство датского Datatilsynet по управлению правами доступа к данным



Датский орган по защите данных (Datatilsynet) 07.12.2023 опубликовал руководство по управлению правами доступа. В руководстве рассматривается концепция управления правами, которая определяется как управление доступом к ИТ-системам и помещениям организации, а также к информации, к которой могут получить доступ отдельные пользователи.

Согласно руководству, управление правами в организации - это коллективная ответственность, включающая в себя различные роли, каждая из которых наделена определенными обязанностями. Обработчики данных и операторы ИТ-систем должны обеспечить настройку ИТ-систем для соблюдения политики управления правами. В то время как DPO отвечают за мониторинг и консультирование по вопросам защиты персональных данных, чтобы предотвратить несанкционированный доступ.

Все сотрудники организации, независимо от их роли в сфере ИТ-безопасности, несут ответственность за осведомленность о своих правах доступа и их соответствие рабочим требованиям.

Технические и организационные меры, которые могут быть реализованы для обеспечения ответственного управления правами:

- многофакторная аутентификация (MFA);
- регистрация доступа пользователей к персональным данным;
- автоматическое управление доступом;
- минимизация прав привилегированного доступа;
- внедрение прав доступа на основе ролей.

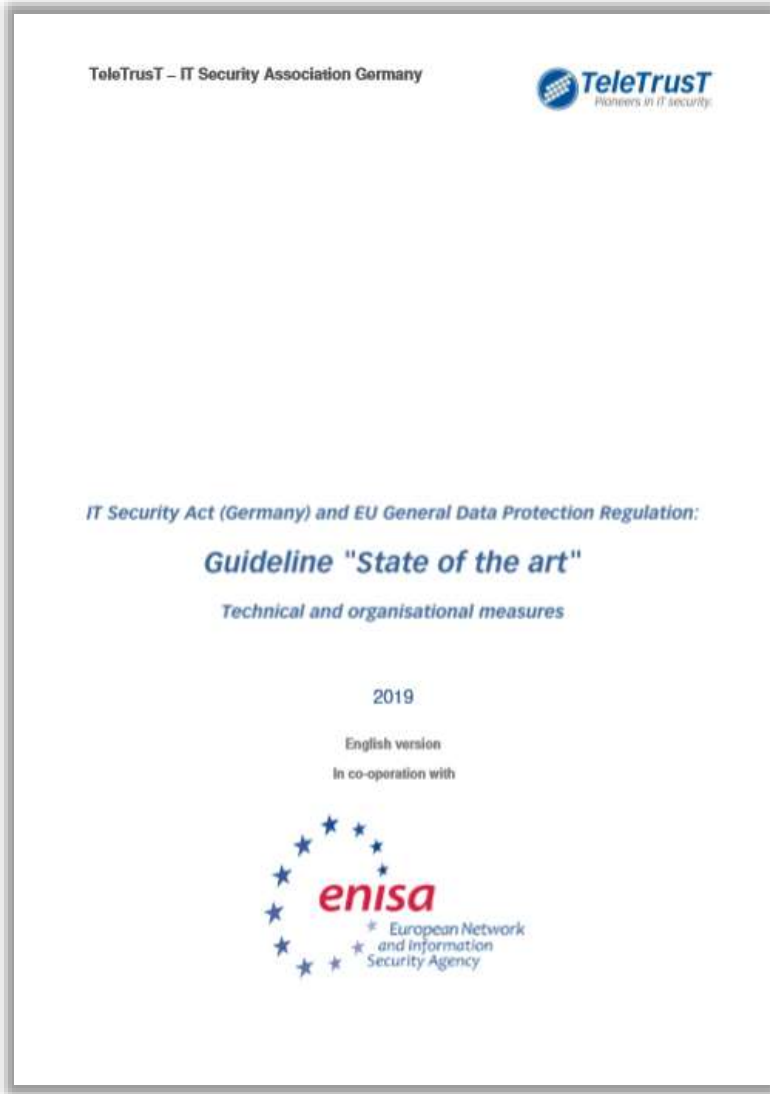
## 491 Руководство итальянских Garante и ACN по хранению паролей



Итальянское агентство национальной безопасности (ACN) и итальянский орган по защите данных (Garante) 12.12.2023 опубликовали руководство по техническим мерам, которые должны быть приняты для хранения паролей. Руководство предназначено для компаний и администраций, которые хранят пароли своих пользователей в своих системах, субъектов, которые получают доступ к базам данных особой важности или размера, или пользователей, которые обрабатывают конфиденциальные или судебные данные.

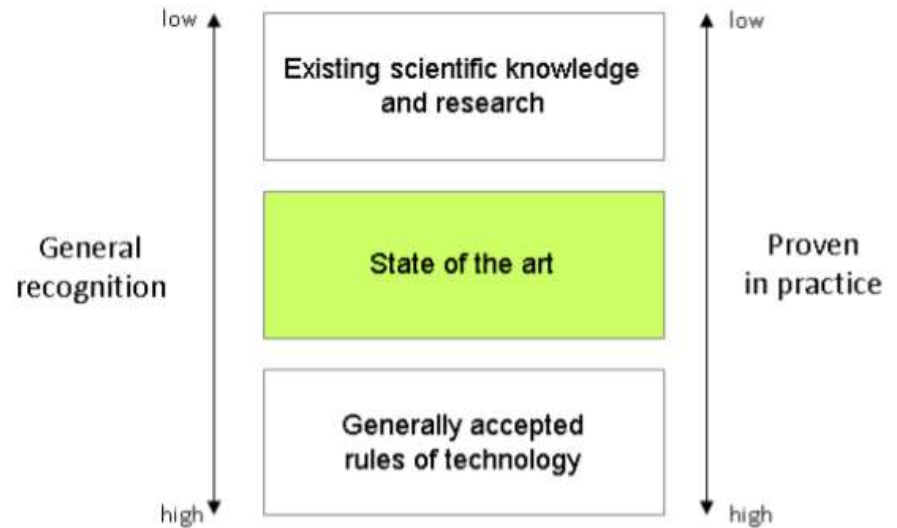
Цель руководства - дать рекомендации по наиболее безопасным техническим функциям, которые должны быть реализованы для хранения паролей.

В руководстве поясняется, что эти меры призваны предотвратить нарушение учетных данных киберпреступниками. Методы и минимальные параметры, о которых идет речь в руководстве, включают, в частности, совершенствование методов хеширования паролей и использование различных алгоритмов.

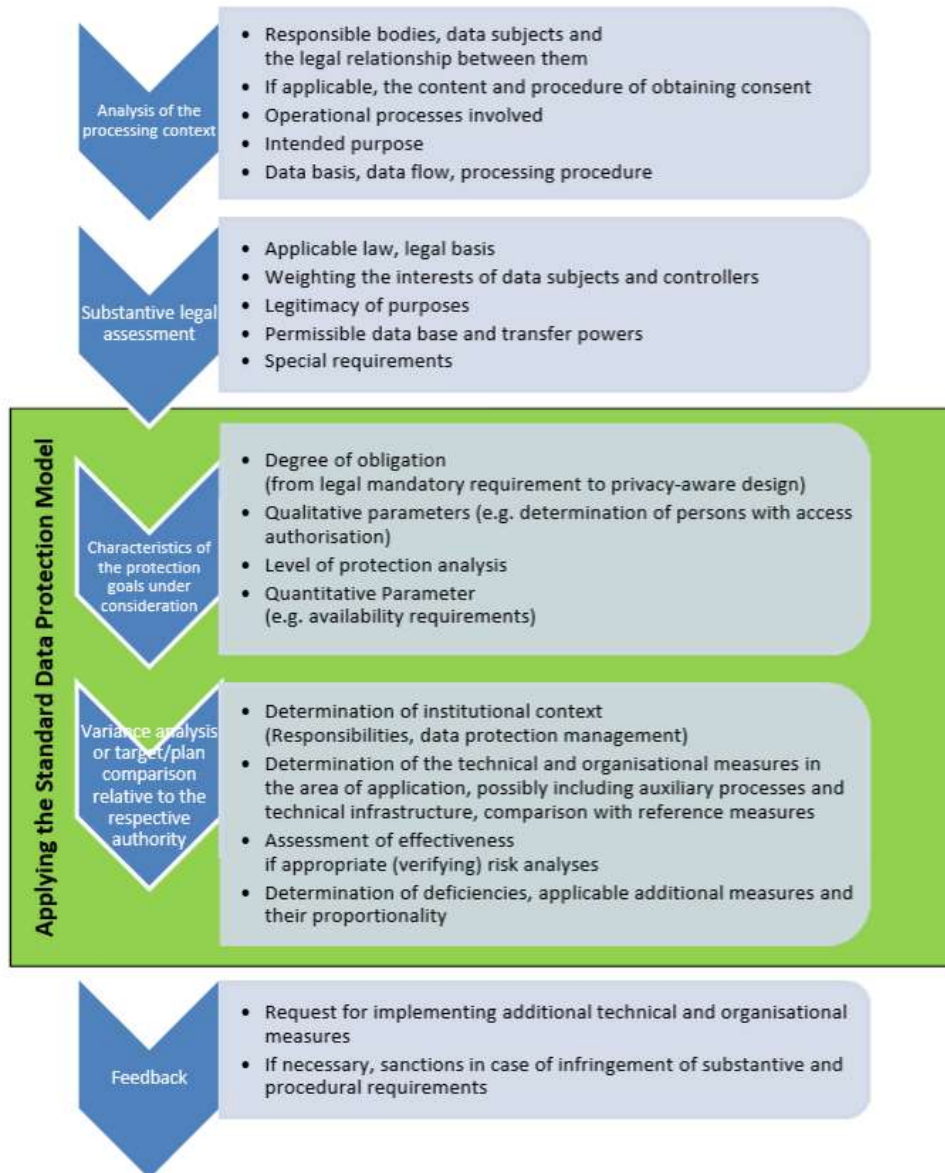


## Bundesverband IT-Sicherheit e.V. (TeleTrust)

В феврале 2019 года Ассоциация ИТ-безопасности Германии подготовила и при поддержке ENISA перевела на английский язык руководство по современному уровню развития (State-of-the-Art) технических и организационных мер защиты информации в части, касающейся требований немецкого закона IT Security Act и европейского GDPR.

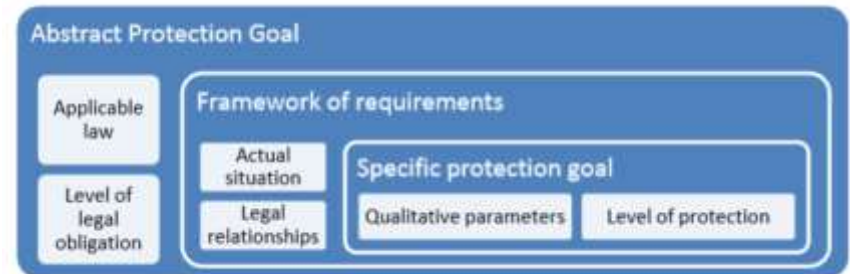


## 493 Standard Data Protection Model



Федеральный уполномоченный по защите данных и свободе информации ("BfDI") опубликовал Стандартную модель защиты данных ("SDM 3.0"), которая была принята немецкой конференцией по защите данных ("DSK"). Целью документа является обеспечение подходящих механизмов для перевода правовых требований GDPR в технические и организационные меры:

- третья (актуальная) версия на [немецком](#);
- вторая (неактуальная) версия на [английском](#).



## Стандарт информационной безопасности немецкого BSI для малого и среднего бизнеса

Standard-Sicherheitscheck für KMU:  
BSI entwickelt mit Partnern DIN-SPEC

Ort Bonn  
Datum 26.04.2023



Quelle: © Fotolia/sdecoret

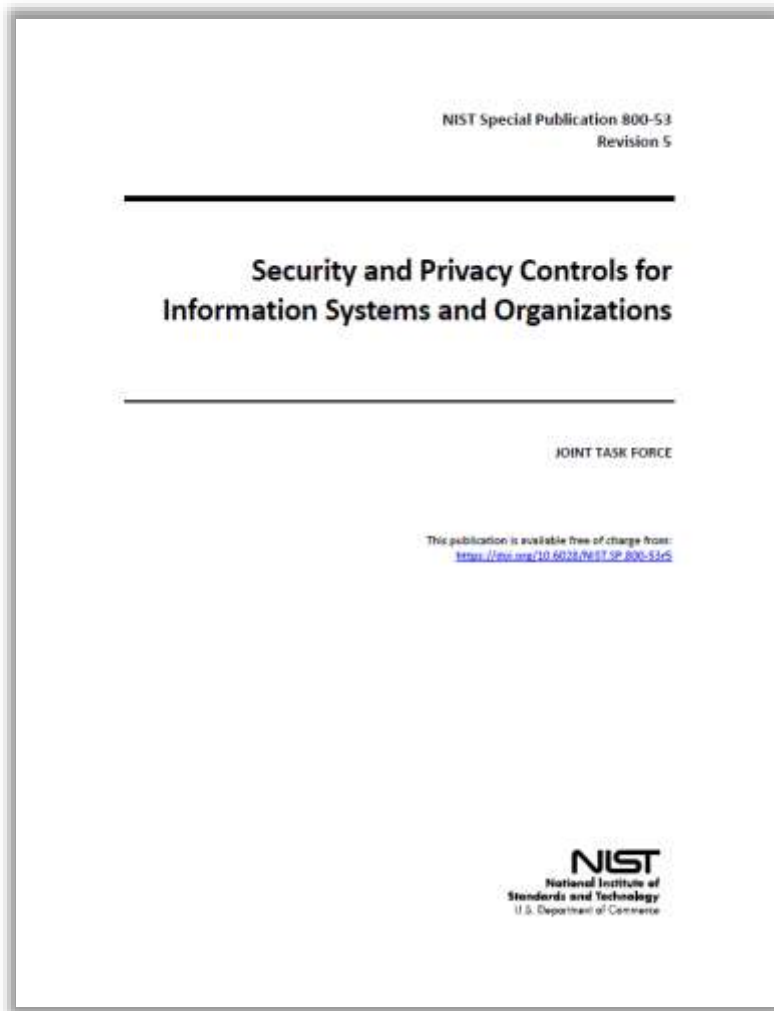
Immer mehr Verantwortliche in kleinen und mittleren Unternehmen (KMU) erkennen, dass sie ohne ihre IT-Systeme nicht mehr arbeitsfähig sind und sie diese daher angemessen schützen müssen. Oftmals wissen sie aber weder, wie gut oder schlecht es um ihre Informationssicherheit konkret bestellt ist, noch welche Wege sinnvollerweise zu gehen sind, um das Schutzniveau zu erhöhen. Abhilfe schafft nun ein neuer Standard für IT-Sicherheitsberatungen, der durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Kooperation mit dem Bundesverband mittelständische Wirtschaft (BVMW) sowie rund 20 weiteren Partnern entwickelt wurde. Damit wird insbesondere KMU der Einstieg in die Informationssicherheit weiter erleichtert.

Der > CyberRisikoCheck nach DIN SPEC 27076 dient der IT-Sicherheitsberatung für kleine Unternehmen. Die Spezifikation gibt vor, wie die Beratung durchzuführen ist und welche Inhalte der Beratungsbericht enthalten muss. Insgesamt müssen im Gespräch mit dem jeweiligen Unternehmen 27 Anforderungen aus sechs Bereichen durch einen

Федеральное ведомство по информационной безопасности ФРГ ("BSI") 26.04.2023 опубликовало стандарт DIN SPEC 27076 "Консультирование по вопросам информационной безопасности для малых и микропредприятий" ("DIN SPEC") и основанной на нем проверки "CyberRisikoCheck", чтобы помочь малым и средним предприятиям ("МСП") начать работу по обеспечению информационной безопасности. DIN SPEC включает стандартизированные рекомендации по действиям для МСП и что с помощью CyberRisikoCheck МСП могут получить стандартизированные рекомендации от поставщиков ИТ-услуг, специально адаптированные к их потребностям.

В рамках CyberRisikoCheck поставщик ИТ-услуг в ходе одно-двухчасового интервью спрашивает компанию о ее ИТ-безопасности, где проверяются 27 требований из шести предметных областей, чтобы выяснить, соответствует ли им компания. Далее BSI пояснил, что в результате соответствующая компания получает отчет, содержащий, помимо прочего, оценку и рекомендации по действиям для каждого невыполненного требования. Кроме того, рекомендации к действию структурированы по степени срочности.

## Руководство по мерам ИБ и приватности для информационных систем и организаций от NIST



Национальный институт стандартов и технологий США опубликовал пятую редакцию своего руководства по мерам ИБ и приватности, которое будет полезно для любой организации или информационной системы, вовлеченной в обработку информации. Документ призван предложить всеобъемлющий и гибкий каталог средств управления ИБ и приватностью для удовлетворения текущих и будущих потребностей в защите информации.

# Чеклисты по проверке уязвимостей в отношении наиболее распространённых нарушений безопасности данных

## CHECKLISTS TO GUARD AGAINST COMMON TYPES OF DATA BREACHES



### CHECKLIST 1

#### Application security in development and support phase

##### OBJECTIVES

This checklist aims to help organisations put in place good practices during their application development phase and support process, to prevent **coding issues** that could result in application errors leading to the subsequent disclosure of personal data. It will also enhance security awareness and responsibilities during coding.

Policy / Risk Management	Practice Met				Action Plan
	Comply	Partial Comply	Not comply	Not Applicable	

##### BASIC PRACTICES

- Develop a Software Development Methodology ("SDM") and perform periodic review for any gaps.
- Develop an IT Change Management Process and perform periodic review for any gaps.

ICT Controls	Practice Met				Action Plan
	Comply	Partial Comply	Not comply	Not Applicable	

##### BASIC PRACTICES

- Conduct code review and rigorous unit testing which includes complete testing of functional requirements to verify the compliance to the requirements specs at early stage in system development lifecycle.



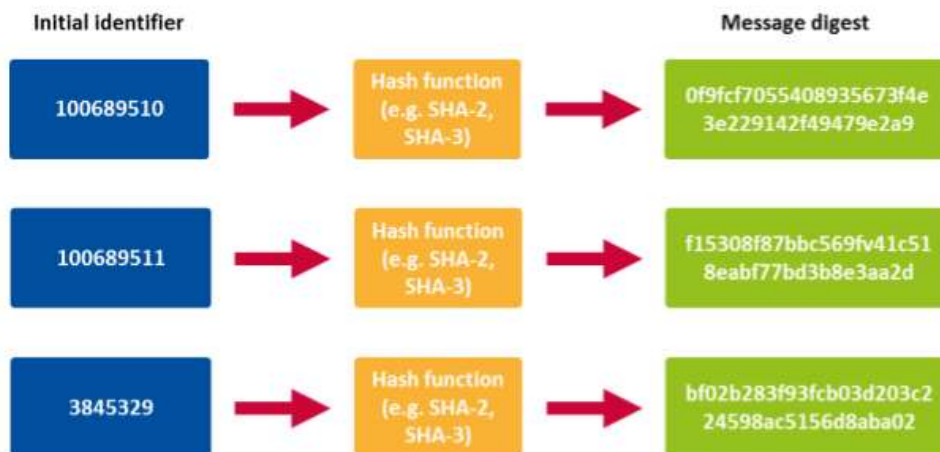
## Псевдонимизация и анонимизация



## Обзор концепции и реализации методов псевдонимизации данных от ENISA



Целью данного обзора является изучение как концепции псевдонимизации, так практической реализации различных методов псевдонимизации данных. Обзор сосредоточен на анализе технических решений для выполнения требований GDPR в части защиты персональных данных и применения концепта «privacy by design».

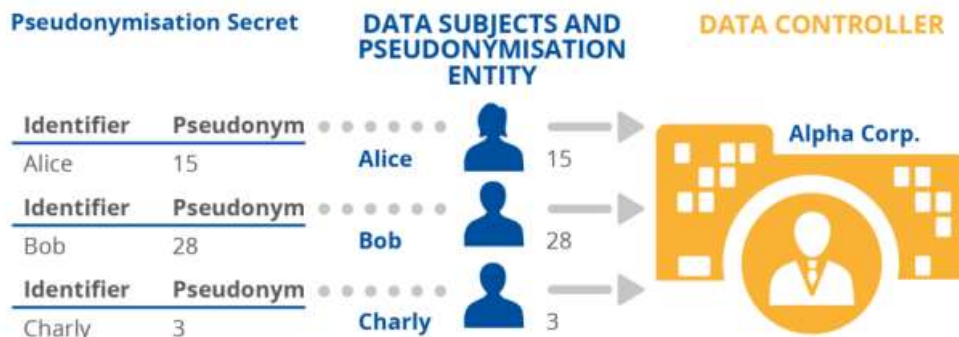


# Рекомендации по техникам псевдонимизации и лучшим практикам от ENISA



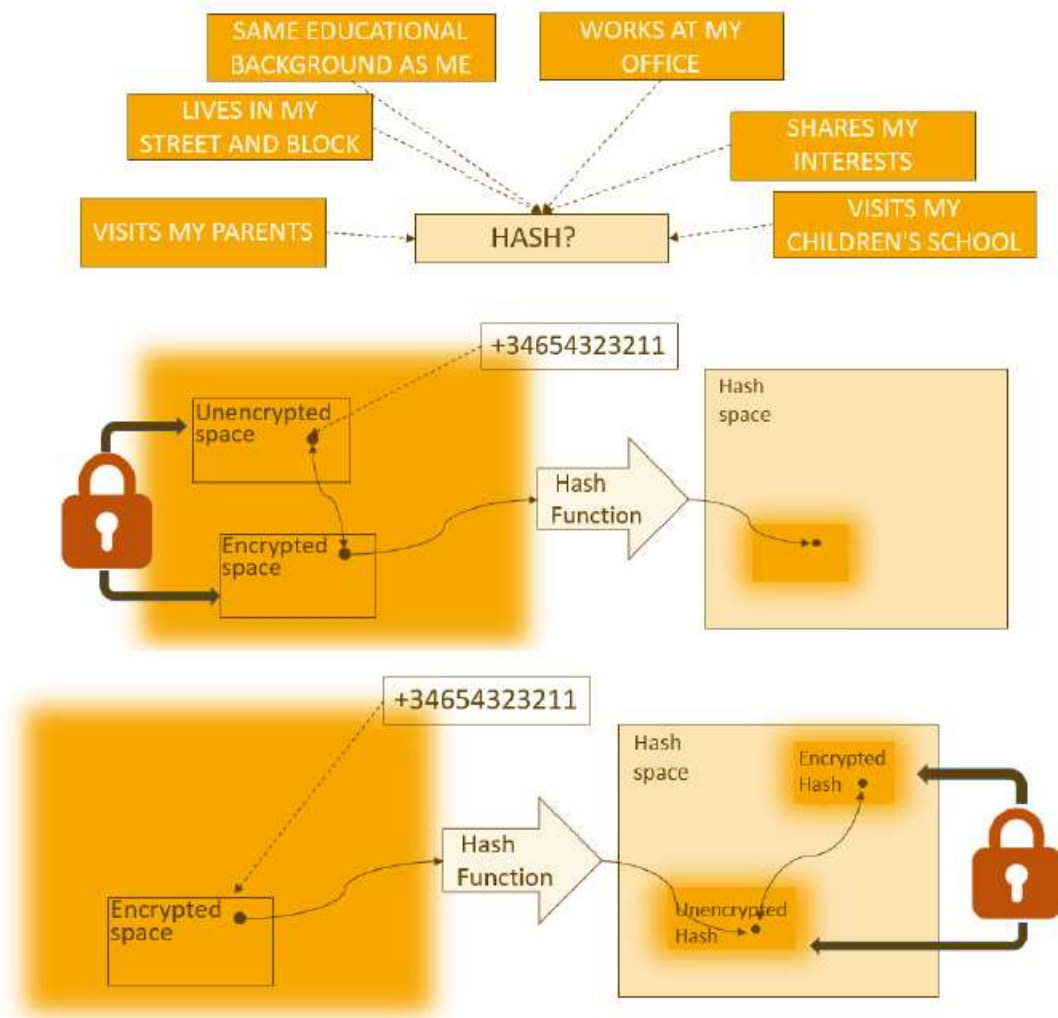
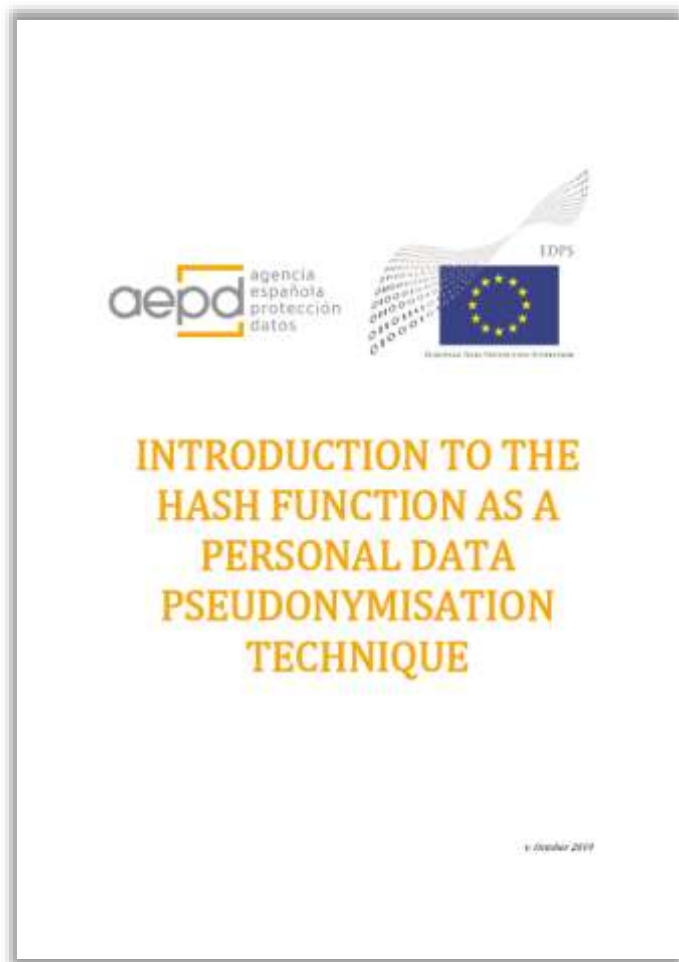
Pseudonymisation Secret

Identifier	Pseudonym
Alice	15
Bob	28
Charly	3
...	...



## Проект руководства ICO по технологиям анонимизации, псевдонимизации и повышения конфиденциальности







The image shows a screenshot of a blog post from the Agencia Española de Protección de Datos (AEPD). The header features the AEPD logo and the text 'agencia española protección datos' next to the Spanish coat of arms. Below the header, the date '23 DE FEBRUARY DE 2023' is displayed. The main title is 'Anonymization III: The risk of re-identification'. The text of the post discusses the requirements for anonymization, emphasizing the need for a formal analysis to ensure that the anonymized data set is not re-identifiable, and the importance of assessing the risk of re-identification and implementing measures to reduce it. Below the text, there are social media sharing icons for Facebook, Twitter, WhatsApp, LinkedIn, and Email. At the bottom of the page, there is a large image showing a silhouette of a person standing in front of a background of glowing blue data points and lines, representing digital data.

agencia española protección datos

23 DE FEBRUARY DE 2023

## Anonymization III: The risk of re-identification

The anonymization is a processing that requires the application of the proactive responsibility principles. This means that the controller must ensure, with a formal analysis, that the anonymized data set is not re-identifiable. However, it must be assumed that there could be a residual probability of re-identification. It is therefore necessary to analyze the impact that re-identification could have on individuals, establish whether additional measures should be implemented to reduce the risk to data subjects, to assess the necessity and proportionality of anonymisation processing, and to conclude whether the anonymisation process offers sufficient guarantees to protect fundamental rights.

— f t w in e



# Руководство AEPD по К-анонимности как способе обеспечения конфиденциальности

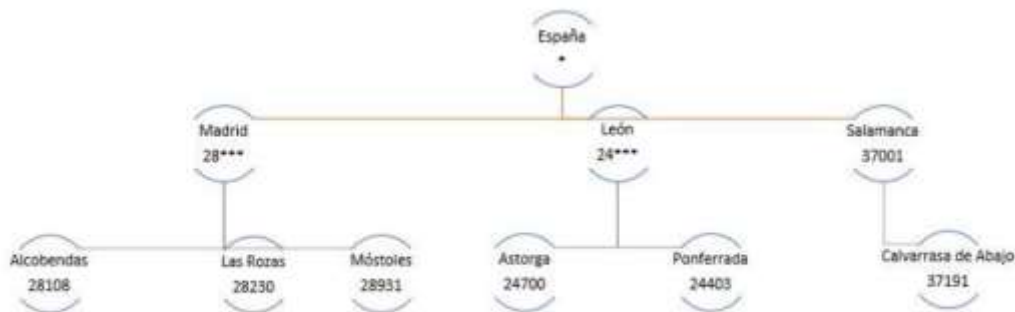
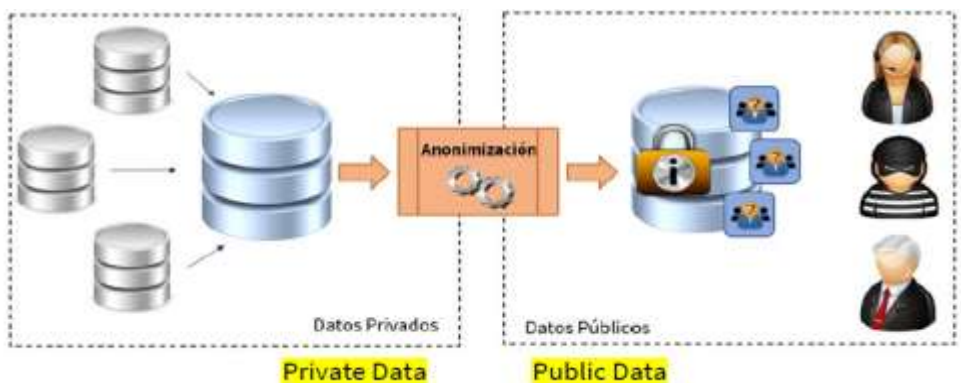


Figure 2: Hierarchy for the Postcode field

Postcode	Age	Cholesterol
37***	40 - 49	Y
28***	40 - 49	Y
24***	30 - 39	N
24***	30 - 39	N
37***	40 - 49	Y
28***	40 - 49	Y

Table 3 - Global generalisation

Postcode	Age	Cholesterol
37***	40 - 49	Y
28***	40 - 49	Y
24700	30 - 39	N
24700	30 - 39	N
37***	40 - 49	Y
28***	40 - 49	Y

Table 4 - Local generalisation

24700	37	N
24700	37	N
37003	44	Y
28108	40	Y
37891	33	N
50011	13	Y

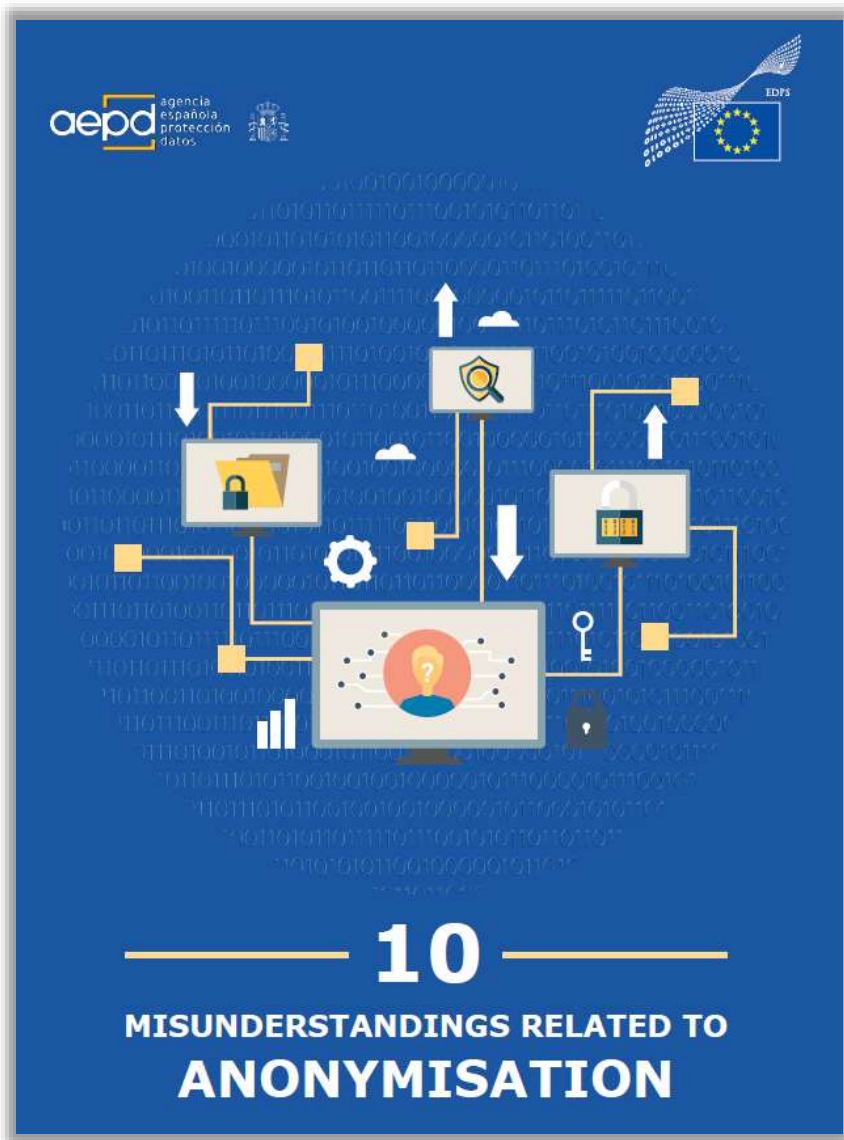
Table 5: Table 2 expanded with data outside the range

Postcode	Age	Cholesterol
37003	40	Y
28108	44	Y
24700	37	N
24700	37	N
37003	44	Y
28108	40	Y
37891	33	N
50011	13	Y

Table 5: Original

Postcode	Age	Cholesterol
37***	40 - 49	Y
28***	40 - 49	Y
24700	30 - 39	N
24700	30 - 39	N
37***	40 - 49	Y
28***	40 - 49	Y
37***	30 - 39	N

Table 6: Generalisation + Suppression on Table 5



EDPS и AEPD опубликовали совместно подготовленный обзор 10 распространенных заблуждений об анонимизации:

1. Псевдонимизация - это то же самое, что и анонимизация
2. Шифрование - это анонимизация
3. Анонимизация данных всегда возможна
4. Анонимизация - это навсегда
5. Анонимизация всегда сводит вероятность повторной идентификации набора данных к нулю
6. Анонимизация - это бинарное понятие, которое невозможно измерить
7. Анонимизация может быть полностью автоматизирована
8. Анонимизация делает данные бесполезными
9. Следование процессу анонимизации, который успешно использовали другие, приведет нашу организацию к эквивалентным результатам
10. Нет никакого риска и никакого интереса в том, чтобы узнать, к кому относятся эти данные



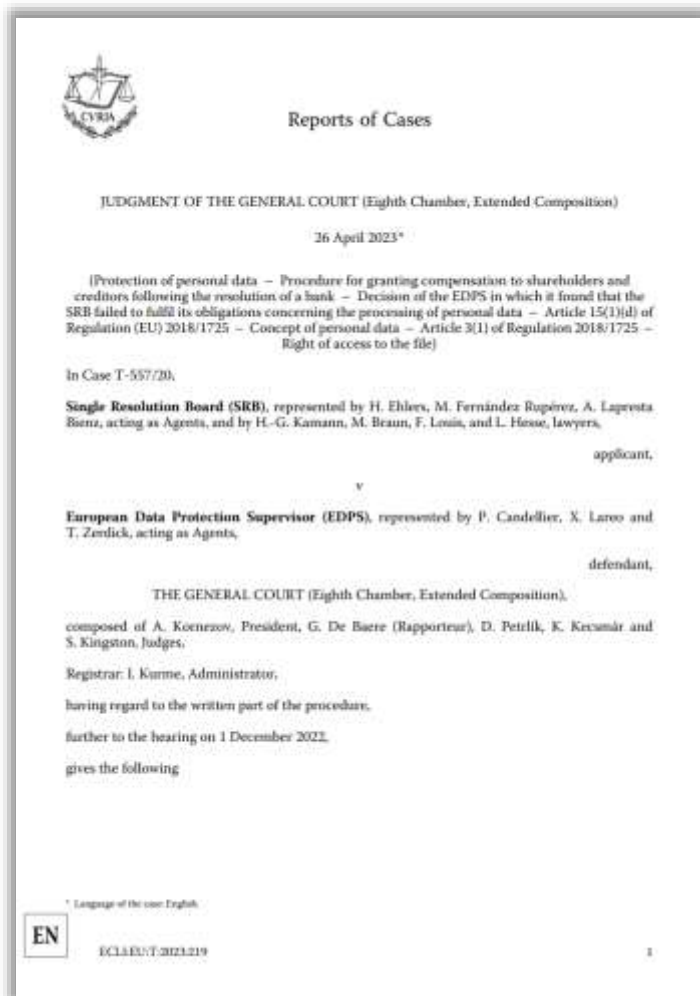
## Позиция BfDI касательно правовых аспектов анонимизации данных с особым вниманием к телеком отрасли



Федеральный комиссар по защите данных и свободе информации в ФРГ опубликовал позицию о правовых аспектах анонимизации данных с особым вниманием к телеком отрасли. В частности, анализируются различные правовое основания для анонимизации персональных данных в зависимости от контекста и цели анонимизации.

Наиболее важный вывод заключается в том, что осуществление анонимизации персональных данных возможно только при соответствующем правовом основании, а в качестве примера приводится телекоммуникационный сектор. Кроме того, BfDI указал, что обязательство по немедленному уничтожению персональных данных может быть реализовано путем анонимизации, выполняемой с учетом самых строгих требований.

## Псевдонимизированные данные, отправленные получателю - не персональные, если получатель не имеет возможности установить субъектов



Нормативное руководство ЕС и прецедентное право CJEU (например, Beyer) всегда устанавливали невозможно высокий стандарт для анонимизации. Однако решение Генерального суда ЕС по делу T-557/20, SRB v EDPS, дает проблеск надежды на то, что анонимизация может быть легче достижима.

Предыстория: SRB обратилась к частным лицам с просьбой представить свои комментарии через электронную форму. Имена были заменены случайным 33-значным буквенно-цифровым кодом. SRB предоставила данные с ключевым кодом третьей стороне. Третья сторона не имела средств для повторной идентификации субъектов данных. EDPS решил, что данные, переданные получателю, являются псевдонимизированными только потому, что SRB располагает дополнительной информацией для декодирования данных. Европейский суд отменил это решение. Основные выводы:

- необходимо учитывать точку зрения получателей данных при рассмотрении вопроса о том, являются ли данные персональными;
- псевдонимизированные данные, переданные получателю, будут анонимными данными, если у получателя нет средств для повторной идентификации субъекта данных;
- тот факт, что отправитель данных имеет средства для повторной идентификации субъектов данных, не имеет значения и не означает, что переданные данные автоматически также являются персональными данными для получателя.

# Рекомендации Архива данных по социальным наукам Финляндии в отношении анонимизации данных

Version 1.0 (12.4.2019) Finnish Social Science Data Archive (FSD)

Dataset name:

Creator(s) of the plan:

Person(s) carrying out anonymisation:

[Factors affecting anonymisation decisions](#) are presented below.

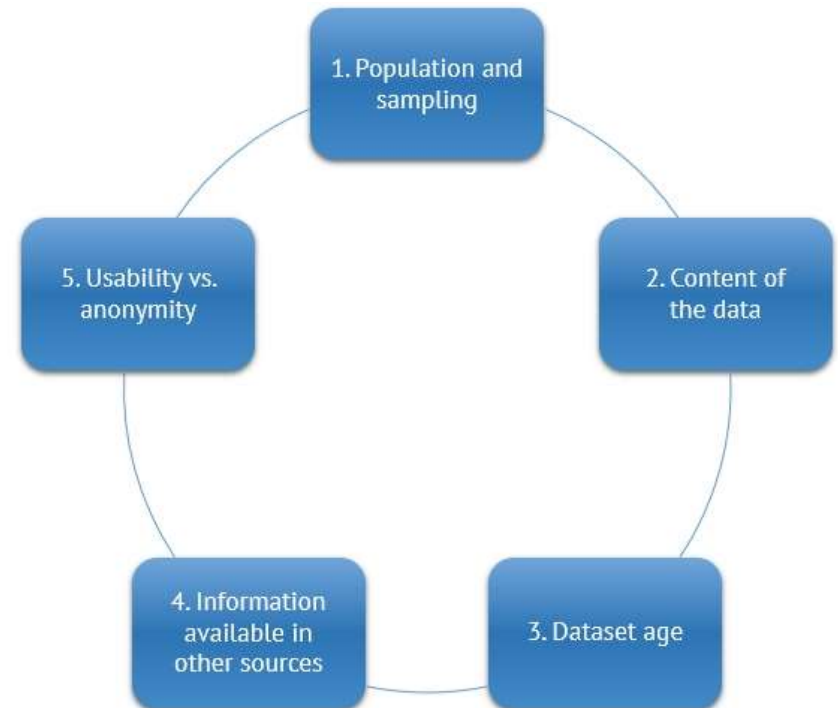
1. **Population and sampling:** *Who were the target population of the study and how was sampling conducted? How many people belonging to the population were included in the sample? What is known about the population beforehand (e.g. distribution of gender and age)? Do individuals belonging to the population share a rare phenomenon?*
2. **Content of the data:**
  - a) *What kinds of direct and indirect identifiers do the data contain? What combinations of information in the data could be used to identify an individual?*
  - b) *Does the dataset contain information related to third persons and can individuals be identified based on this information?*
  - c) *Does the dataset contain exceptional or unique information?*
  - d) *Does the dataset contain sensitive information?*
3. **Dataset age:** *Have the data of the population in the dataset changed over time?*
4. **Information on the respondents available in other sources:** *Is it possible to connect the information in the data to information from other sources? Is it possible to identify individuals based on information available in other sources?*
5. **Usability vs. anonymity:** *What types of information in the data are the most significant with regard to research, i.e. what information must be preserved during anonymisation and what information can be removed?*

**Anonymisation decisions:**


*What is removed, categorised, coarsened? Quantitative datasets: How are open-ended responses processed? Note that any documents relating to anonymisation cannot contain pseudonymous information or other information based on which individuals could still be identified. For instance, lists of aliases/pseudonyms used for personal names must be destroyed when they are no longer needed.*

**Rationale for anonymisation and assessing disclosure risk after anonymisation:**

*Provide rationale for anonymisation solutions and policies. Assess the possibility of identifying individuals in the data now and in the future. Think about when the anonymity of the data should be reviewed again (residual risk assessment). You can also provide further information regarding, for instance, the anonymisation process, how anonymisations are marked, and possible errors that secondary users of the data should take into account.*



**DPOrganizer**



BLOG POST

### A winding road through 'anonymisation' legal landscape

KONSTANTIN TIAZHELMIKOV

AUGUST 31, 2022 - 6 MIN READ

Under the GDPR Recital 26, anonymous information is 'information which does not relate to an identified or identifiable natural person' or 'personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'. Anonymous personal data is outside the scope of the GDPR, thus making its rules inapplicable. This explains why decent anonymisation techniques are indeed in great demand in different companies and organisations.

With that said, the GDPR does not itself explain how to make the data subject 'no longer identifiable' and what really stands behind this concept.

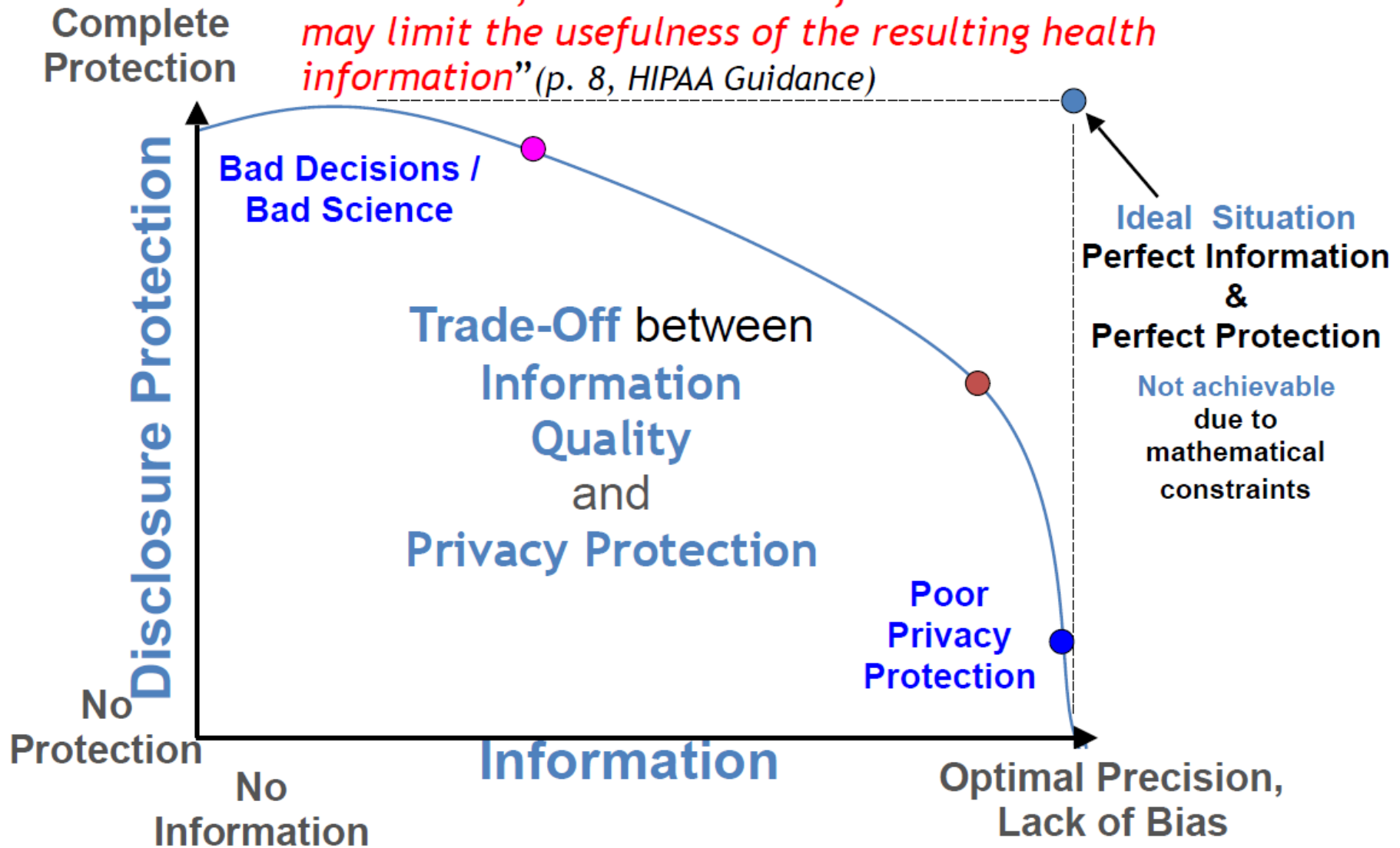
Согласно статье 26 GDPR, анонимная информация - это "информация, не относящаяся к идентифицированному или идентифицируемому физическому лицу" или "персональные данные, обезличенные таким образом, что субъект данных не идентифицируется или более не идентифицируется".

Анонимные данные находятся вне сферы действия GDPR, что делает его правила неприменимыми. Это объясняет, почему достойные методы анонимизации действительно пользуются большим спросом в различных компаниях и организациях.

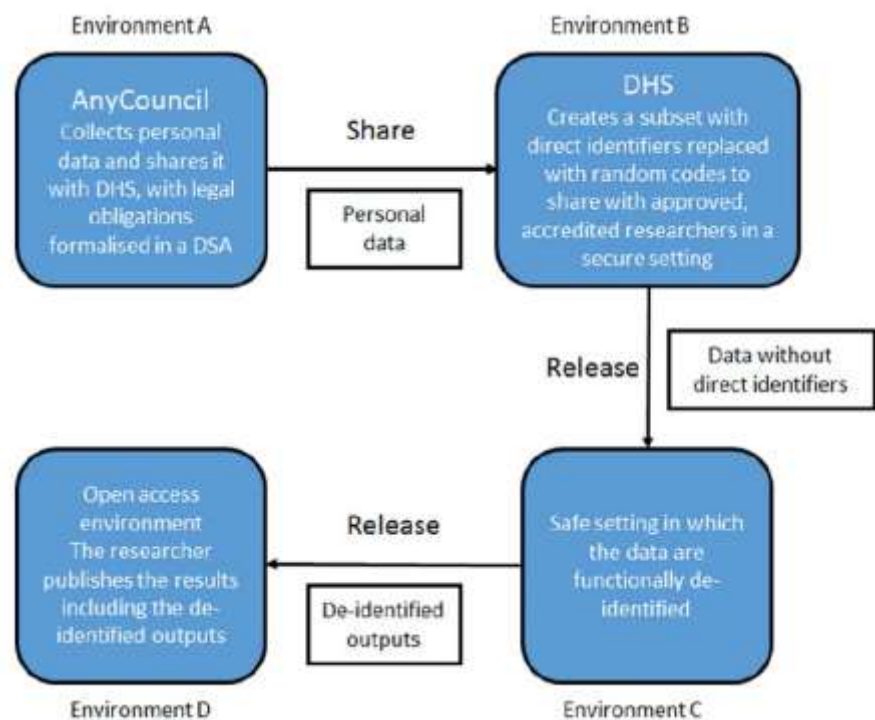
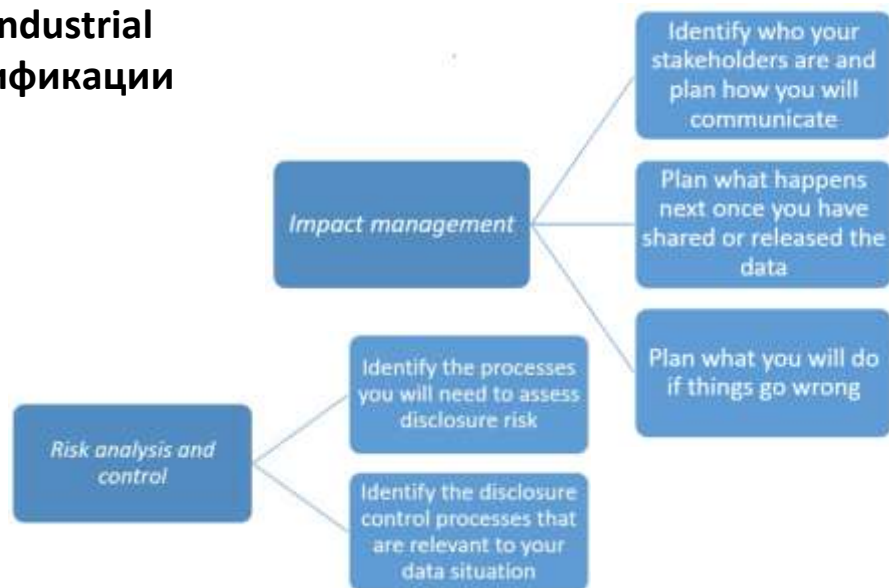
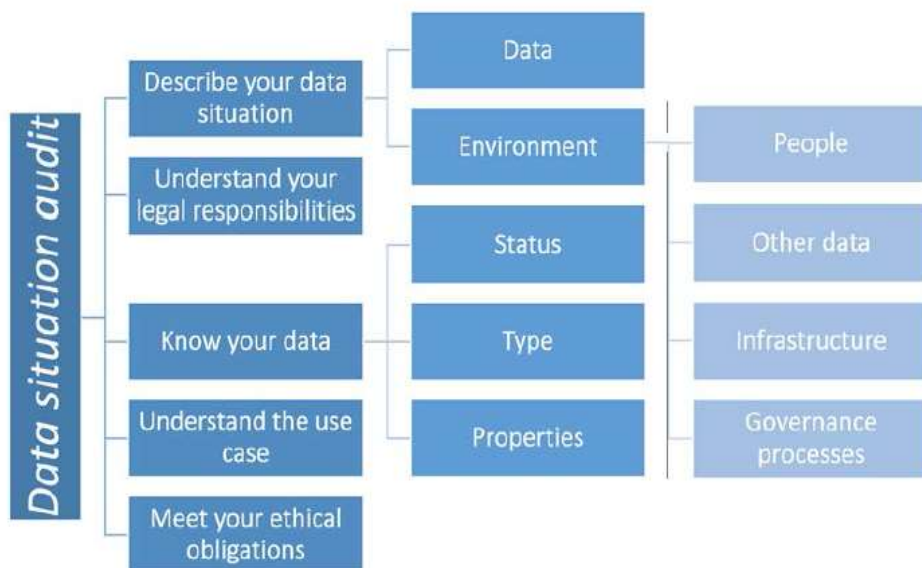
При этом GDPR сам по себе не объясняет, как сделать субъекта данных "более не идентифицируемым" и что на самом деле стоит за этим понятием.

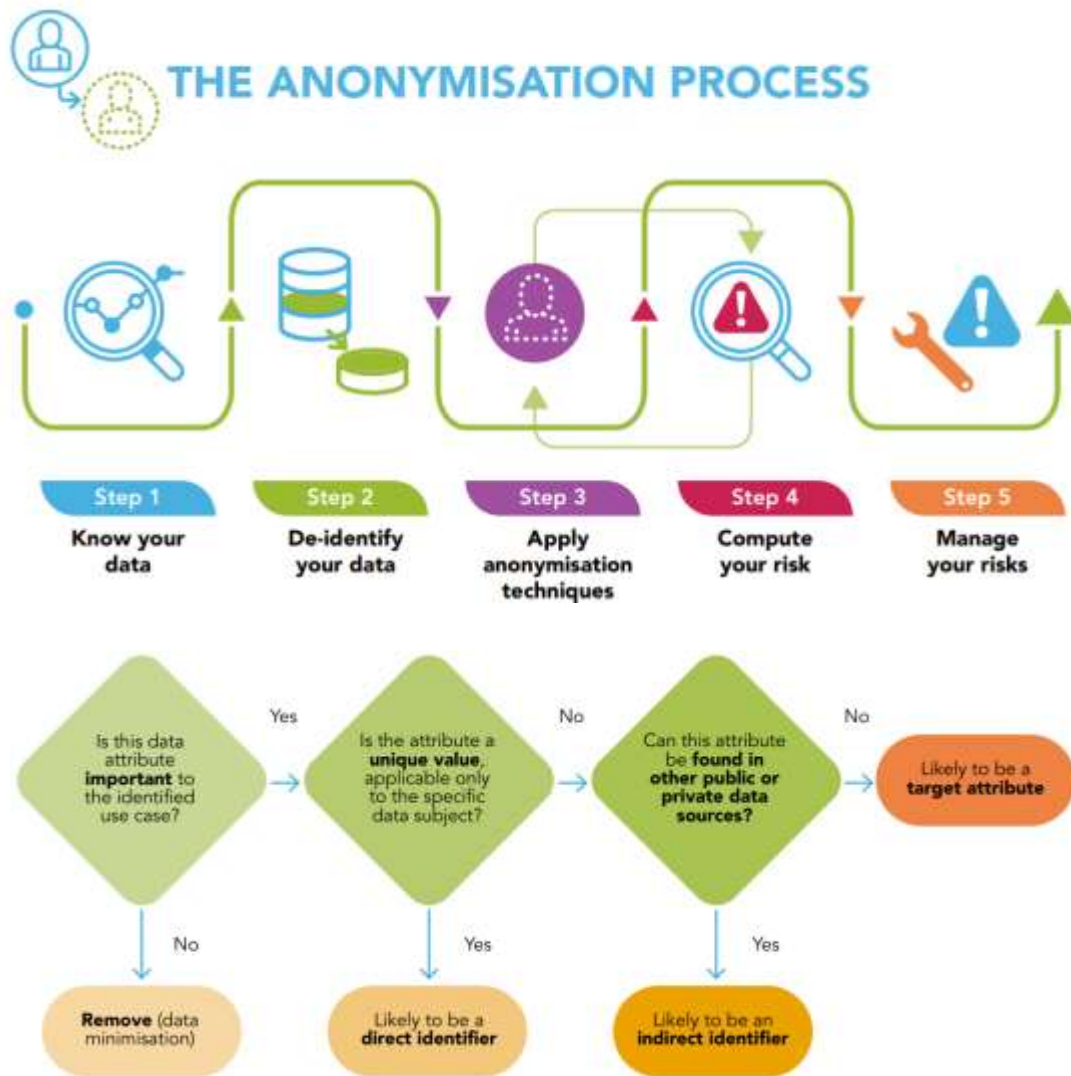
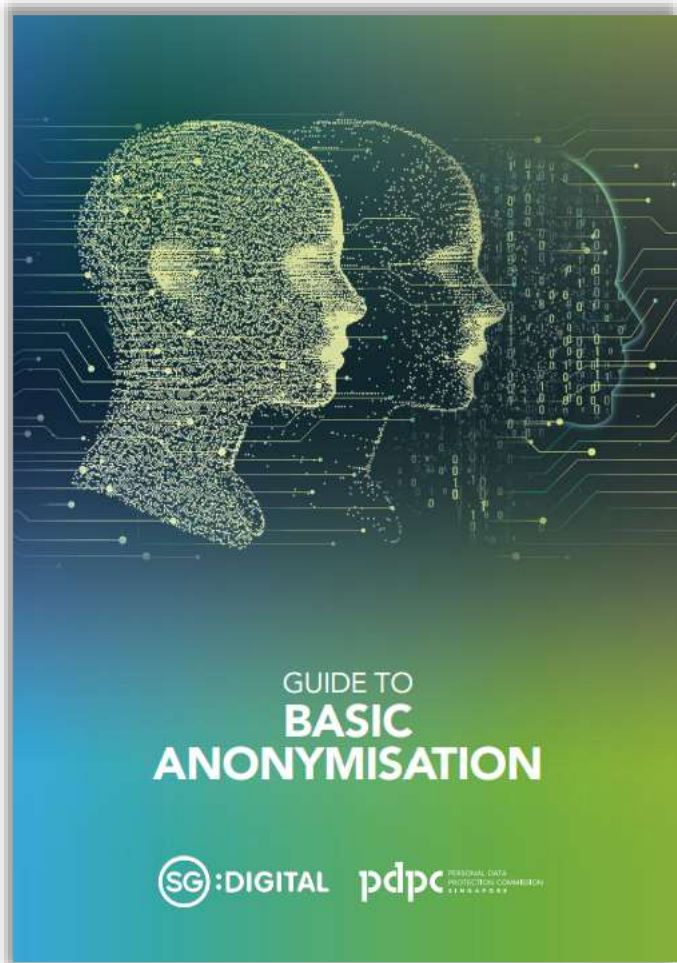
Если говорить о "мягком праве", то оно постоянно менялось на протяжении многих лет: в 2007 и 2014 годах Рабочая группа 29 (WP29) придерживалась несколько разных подходов к анонимизации, а EDPB иногда делилась лишь точечными разъяснениями. В свою очередь, национальные надзорные органы занимали противоречивые позиции, склоняясь либо к подходу 2007 года, либо к подходу 2014 года.

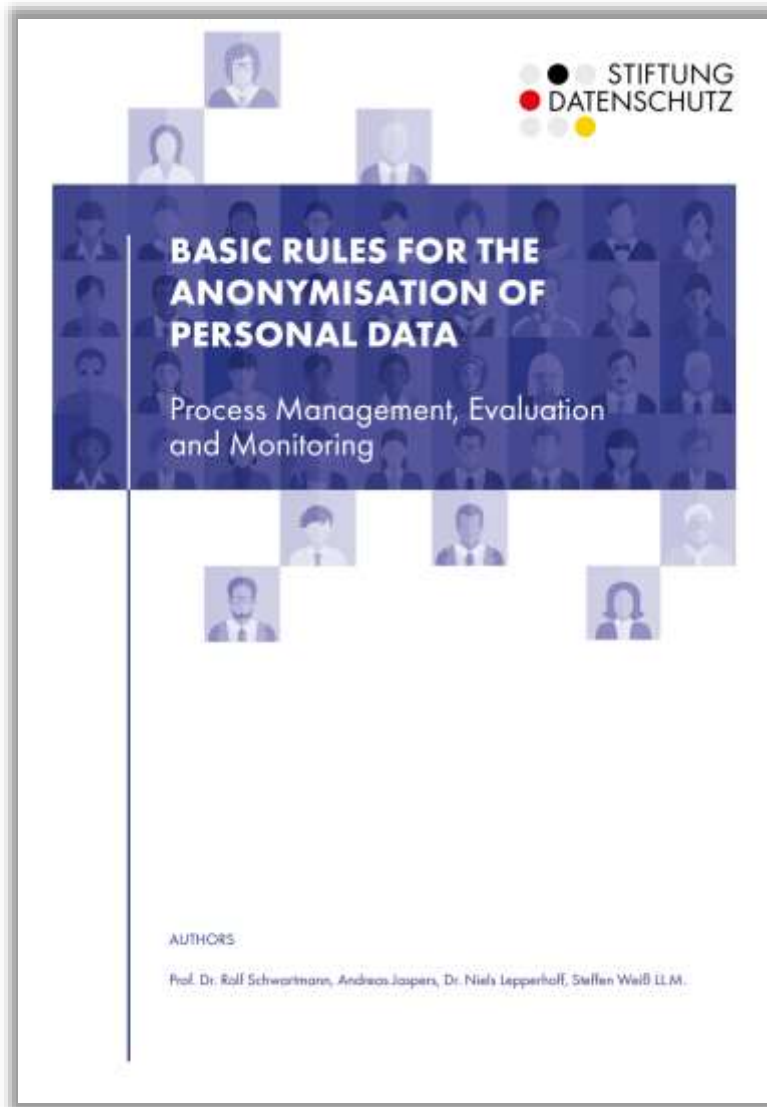
*“De-identification leads to information loss which may limit the usefulness of the resulting health information” (p. 8, HIPAA Guidance)*



## Методология от Commonwealth Scientific and Industrial Research Organisation (Австралия) по деидентификации



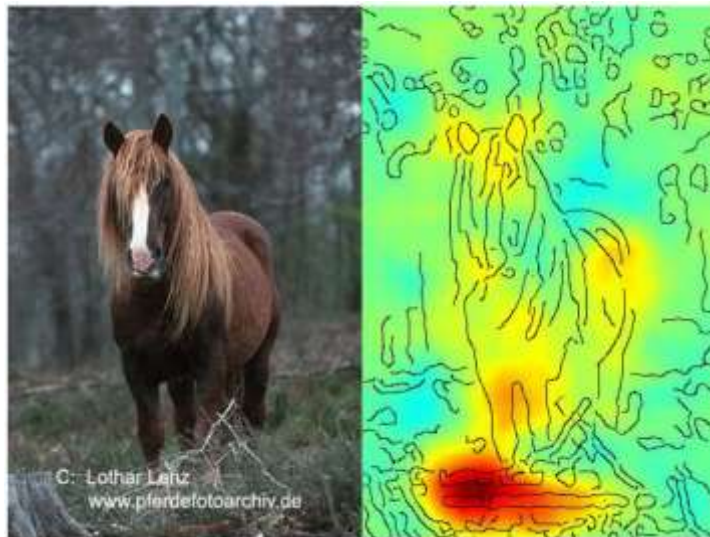
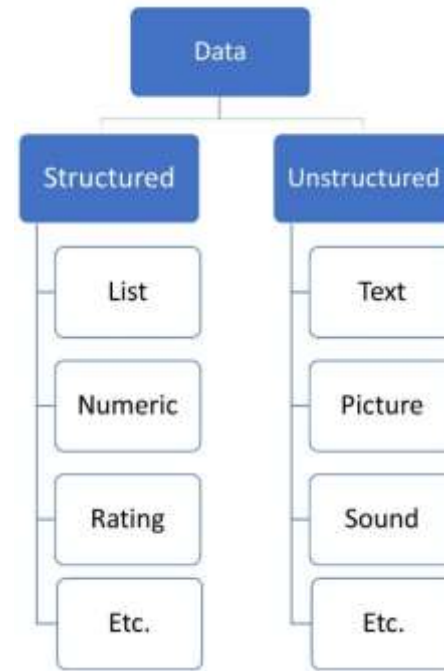
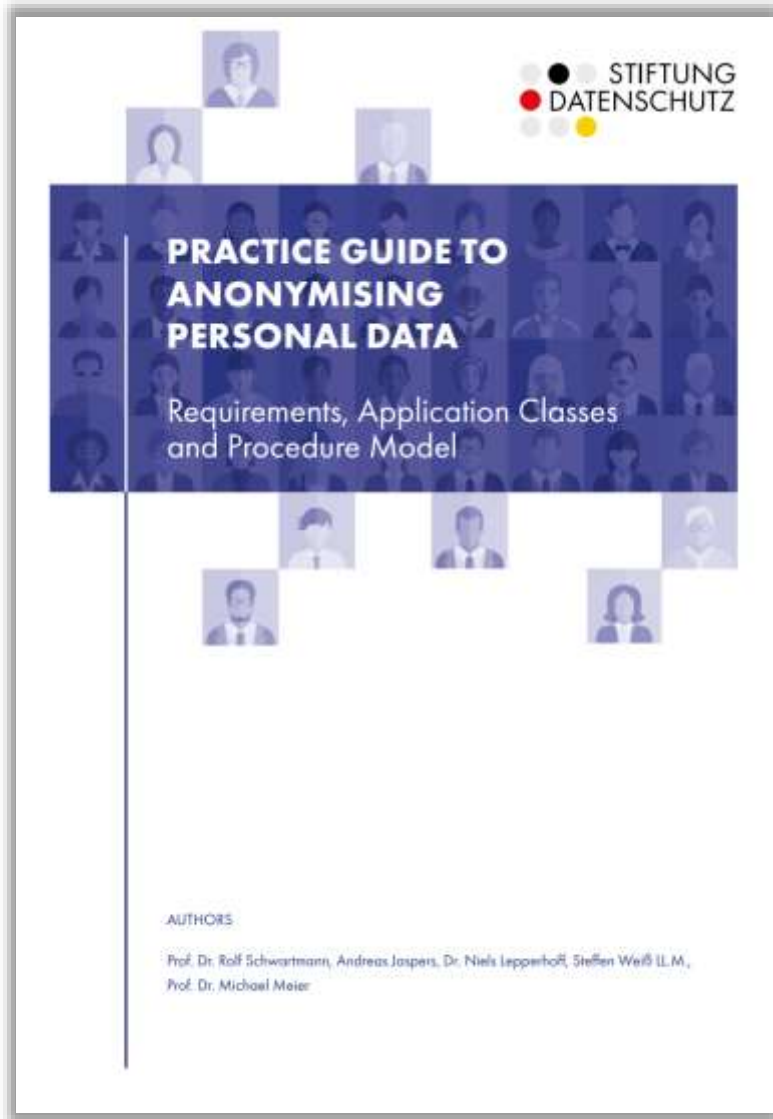




1. AIM .....	1
2. GENERAL DEFINITIONS OF TERMS .....	1
3. SCOPE OF APPLICATION OF THE BASIC RULES .....	1
4. REQUIREMENTS TO BE MET .....	2
4.1 Organisational measures .....	2
4.2 Identification and documentation of the criteria necessary to determine the anonymisation method.....	2
4.3 Conducting the anonymisation .....	4
4.4 Disclosure of anonymised data to third parties .....	4
4.4.1 General requirements.....	5
4.4.2 Joint controllership .....	5
4.5 Rights and role concept.....	6
4.6 Principles relating to processing of personal data.....	6
4.7 Unintentional/unlawful re-identification of data subjects.....	6
4.8 Documentation .....	7
4.9 Attacker model .....	7
4.10 Regular review .....	8
5. MONITORING BY THE MONITORING BODY .....	8
5.1 Duty to cooperate .....	8
5.2 Cooperation obligations of other controllers and processors .....	9
5.3 Powers of the monitoring body.....	9
5.3.1 Process: Control of the voluntary commitment.....	10
5.3.2 Process: Sanctions for violation of the voluntary commitment.....	11
5.4 Process: Review for breach of self-commitment in case of complaint .....	13
5.5 Process: Informing the supervisory authority in the event of withdrawal of the voluntary commitment.....	15
5.6 Process: Publication of obligated companies.....	16
5.7 Process: Publication of suspended or withdrawn voluntary commitments. ....	16
6. PROCESS: REVIEW OF THE BASIC RULES .....	16



## 513 Практическое руководство по анонимизации



# A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION



What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.



## DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.



## PSEUDONYMOUS DATA

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.



## DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.



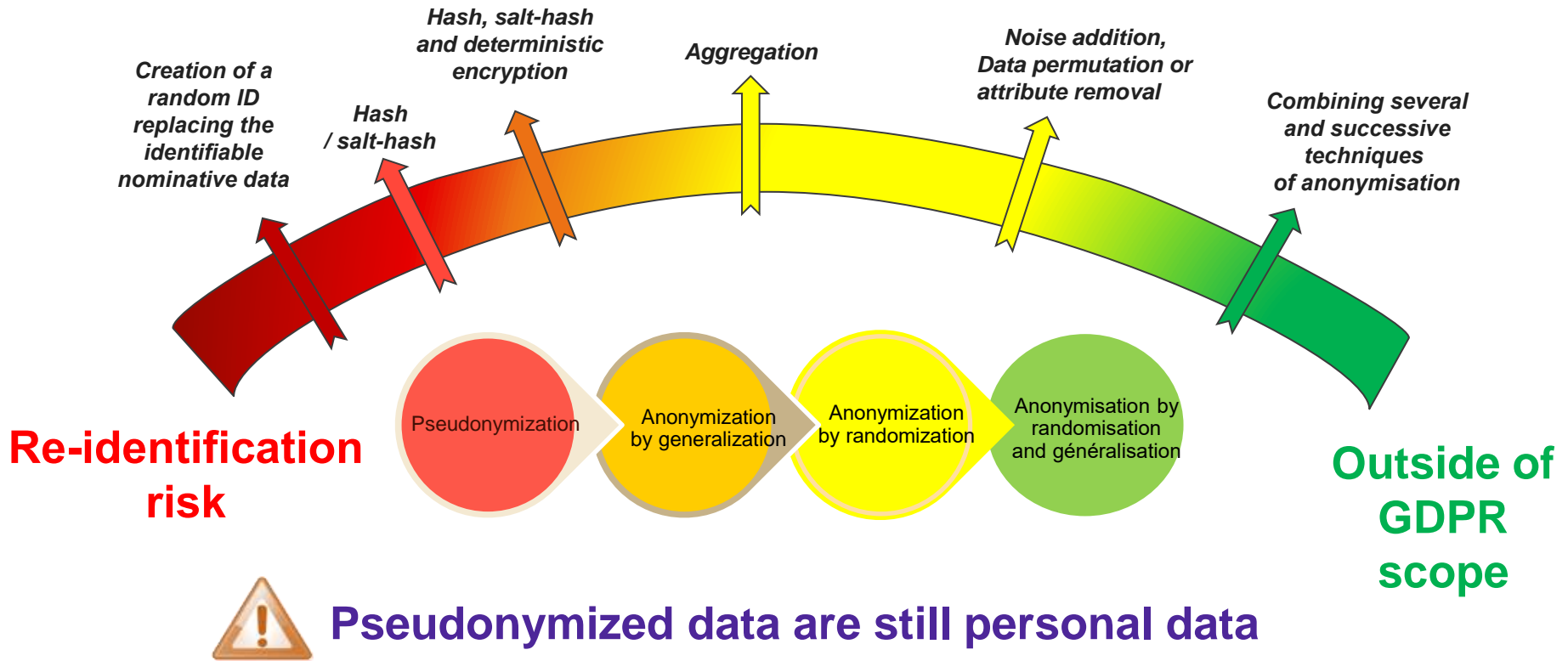
## ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

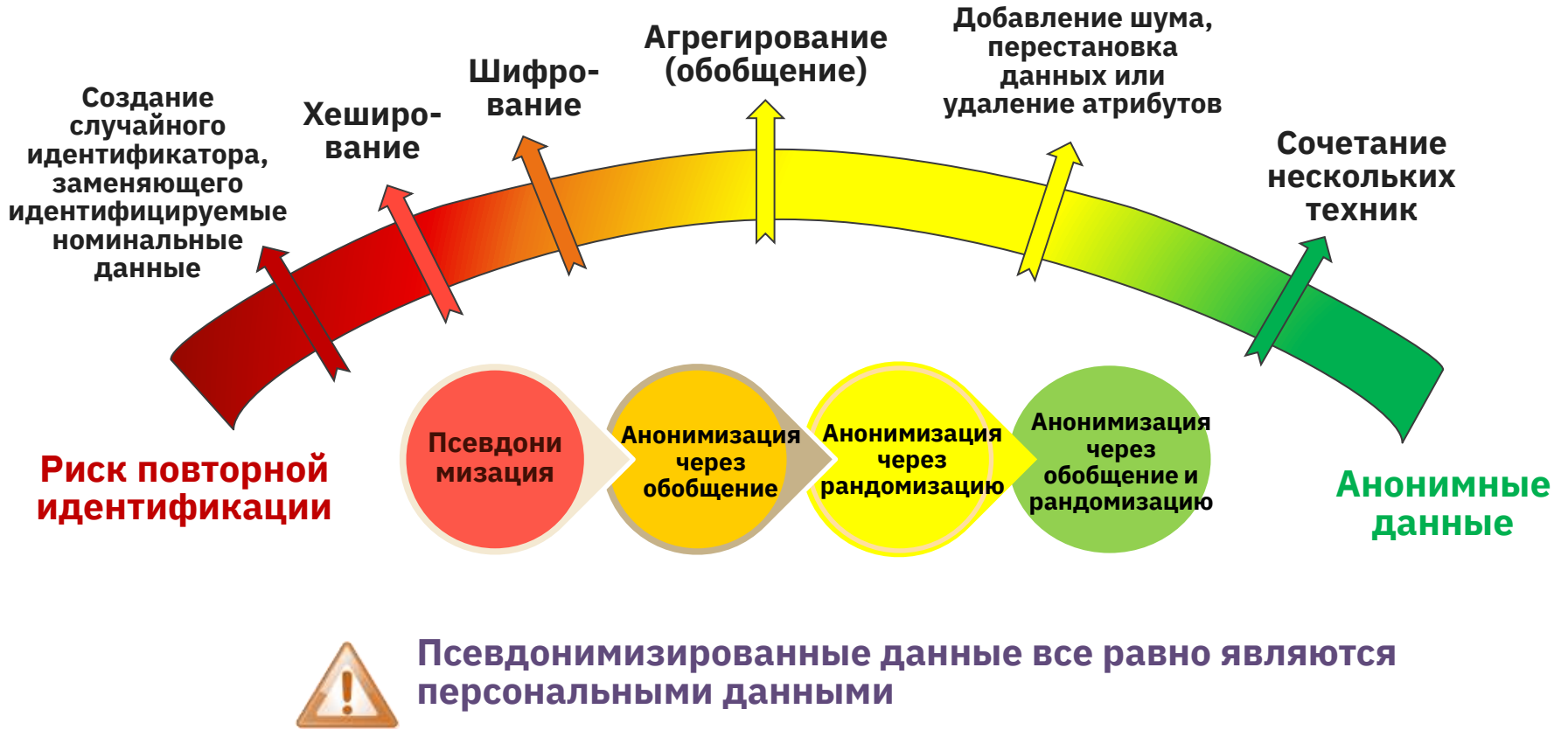
This is a primer on how to distinguish different categories of data.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
<b>DIRECT IDENTIFIERS</b> Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
<b>INDIRECT IDENTIFIERS</b> Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
<b>SAFEGUARDS and CONTROLS</b> Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation
<b>SELECTED EXAMPLES</b>	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 333-333-3333)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68-AR-6D-35-95-03)	Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 1S.1 g/dl = Csk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = S17TJK619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)	Same as De-identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)

## WHAT IS NOT PERSONAL DATA: ANONYMISATION



516 От псевдонимизации к анонимизации персональных данных в GDPR



## Территориальная сфера действия GDPR



Требования Регламента Европейского союза по защите персональных данных не будут распространяться на российских операторов, работающих в России – А. Жаров

9 ноября 2017 года <https://rkn.gov.ru/news/rsoc/news51780.htm>



Требования вст  
Европейского с  
будут распро  
осуществляющ  
них распростра  
сфере. Об этом  
Александр Жар  
VIII Междунаро  
данных».

По его словам,  
участницей ме

устанавливающих порядок обработки персональных данных и  
«Регламент, по нашему мнению, должен учитываться только по  
европейских граждан российскими операторами на территории  
отметив, что такая позиция соответствует общепринятым меж  
персональных данных. «Считаю, что к вопросу о применимости  
будет вернуться только после его вступления в законную силу,  
правоприменения. И когда это будет зафиксировано в междуна  
подчеркнул А. Жаров.

Конференция «Защита персональных данных» проводится по  
– уполномоченного органа по защите прав субъектов персона

Состоялось завершающее в 2017 году заседание Консультативного совета при Уполномоченном органе по защите прав субъектов персональных данных

20 декабря 2017 года <https://rkn.gov.ru/news/rsoc/news53394.htm>



Консультативный совет при Уполномоченном органе по защите прав субъектов персональных данных в 2018 году планирует представить предложения по правовому статусу «обезличенных» данных, а также по возможной корректировке законодательства о персональных данных в контексте реализации программы «Цифровая экономика».

Соответствующие решения приняты Советом на последнем заседании в 2017 году, состоявшемся в Роскомнадзоре.

В ходе заседания члены Консультативного совета обсудили новые требования Европейского союза, закрепленные Общим регламентом по защите данных (General Data

Protection Regulation, GDPR), устанавливающим порядок обработки персональных данных. В ноябре на VIII Международной конференции «Защита персональных данных» руководитель Роскомнадзора Александр Жаров отметил, что требования Регламента Европейского союза по защите персональных данных не будут распространяться на российских операторов, осуществляющих деятельности на территории России, поскольку Российская Федерация не является участницей международных договоров с ЕС. На них распространяется действие только российских законов в этой сфере в соответствии с общепринятыми международными принципами обработки персональных данных.

В рамках подведения итогов года на заседании было отмечено участие Консультативного совета в подготовке Методических рекомендаций по разработке отраслевого кодекса поведения в области защиты прав субъектов персональных данных, а также рекомендаций по составлению документа, определяющего политику оператора в отношении обработки персональных данных.

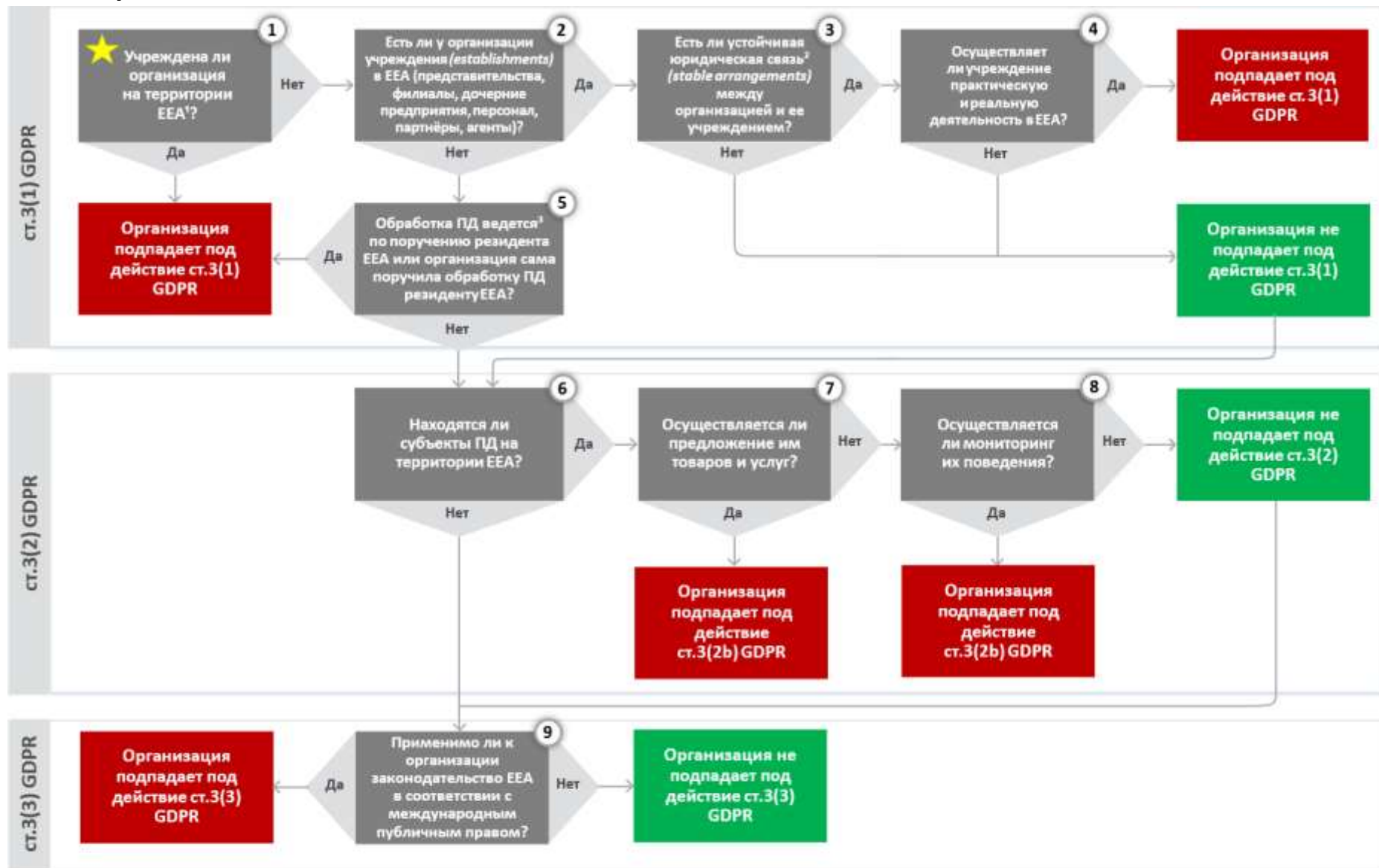


## ЧТОБЫ ПОНЯТЬ, РАСПРОСТРАНЯЕТСЯ ЛИ GDPR на деятельность вашей компании, нужно ответить на следующие вопросы:

- ★ Есть ли у компании представительства (филиалы) на территории Европейского Союза?
- ★ Обработываете ли вы персональные данные граждан стран-участниц Европейского Союза по поручению европейского оператора?
- ★ Руководствуетесь ли при осуществлении деятельности по обработке персональных данных законодательством Европейского Союза или страны-участницы Европейского Союза?
- ★ Осуществляете ли отдельные виды обработки персональных данных европейских граждан, в частности хранение, накопление, с использованием технических мощностей, находящихся на территории Европейского Союза?

**Если вы ответили «ДА» хотя бы на один вопрос, то с большой вероятностью можно сказать, что на деятельность вашей компании GDPR все же распространяется.**

## Определение применимости GDPR к обработке персональных данных



<sup>1</sup> – территория государств-членов Европейской экономической зоны (EEA), когда входят государства ЕС, Исландия, Лихтенштейн, Норвегия, за исключением Швейцарии и Великобритании.

<sup>2</sup> – наличие правоотношений, вне зависимости от их формы (соглашения, контракты, участие в уставном капитале и т.д.).

<sup>3</sup> – обработка ПД, выполняемая на основании и для исполнения договора между оператором и обработчиком (Controller-to-Processor Agreement), ведется в контексте практической и реальной деятельности организации, находящейся в статусе оператора или обработчика, на территории EEA. Применимость GDPR определяется отдельно для каждого факта поручения обработки ПД и не зависит от места фактического осуществления обработки ПД (на территории EEA или вне неё).



## 521 Определение применимости GDPR к обработке персональных данных – перечень вопросов

Определение наличия признаков применимости норм GDPR в отношении тех или иных процессов обработки ПД в организации может быть выполнено посредством последовательного выбора ответов на вопросы закрытого типа.

№	Вопрос	Ответ	GDPR <sup>3</sup>	3/2018 <sup>4</sup>	5/2021 <sup>5</sup>	
1	Учреждена ли организация на территории EU/EEA?	Да – <b>GDPR применим</b> Нет – см. вопрос 2	ст.3(1) гс.22	п.1(a) exp.1	п.13,16, 18 exp.3-4, 6-7	
2	Есть ли у организации учреждения (establishments) в EU/EEA (представительства, филиалы, дочерние предприятия, персонал, партнёры, агенты)?	Да – см. вопрос 3 Нет – см. вопрос 5				
3	Есть ли устойчивая юридическая связь <sup>1</sup> (stable arrangements) между организацией и ее учреждением?	Да – см. вопрос 4 Нет – см. вопрос 6				
4	Осуществляет ли учреждение практическую и реальную деятельность в EU/EEA?	Да – <b>GDPR применим</b> Нет – см. вопрос 6				п.1(b) exp.2-3
5	Обработка ПД ведется <sup>2</sup> по поручению резидента EU/EEA или организация сама поручила обработку ПД резиденту EU/EEA?	Да – <b>GDPR применим</b> Нет – см. вопрос 6				п.1(c),(d) exp.4-7
6	Находятся ли субъекты ПД на территории EU/EEA?	Да – см. вопрос 7 Нет – см. вопрос 9	ст.3(2) гс.14	п.2(a) exp.8-12	п.18 exp.7	
7	Осуществляется ли предложение товаров и услуг субъектам ПД на территории EU/EEA?	Да – <b>GDPR применим</b> Нет – см. вопрос 8	ст.3(2a) гс.23	п.2(b) exp.13-16		
8	Осуществляется ли мониторинг поведения субъектов ПД на территории EU/EEA?	Да – <b>GDPR применим</b> Нет – см. вопрос 9	ст.3(2b) гс.24	п.2(c),(d) exp.17-21		
9	Применимо ли к организации законодательство EU/EEA согласно международному публичному праву?	Да – <b>GDPR применим</b> Нет – <b>GDPR не применим</b>	ст.3(3) гс.25	п.3 exp.22-23	-	

<sup>1</sup> Наличие правоотношений, вне зависимости от их формы (соглашения, контракты, участие в уставном капитале и т.д.).

<sup>2</sup> Обработка ПД, выполняемая на основании и для исполнения договора между оператором и обработчиком (Controller-to-Processor Agreement), ведется в контексте практической и реальной деятельности организации, находящейся в статусе оператора или обработчика, на территории EU/EEA. Применимость GDPR определяется отдельно для каждого факта поручения обработки ПД и не зависит от места фактического осуществления обработки ПД (на территории EU/EEA или вне неё).

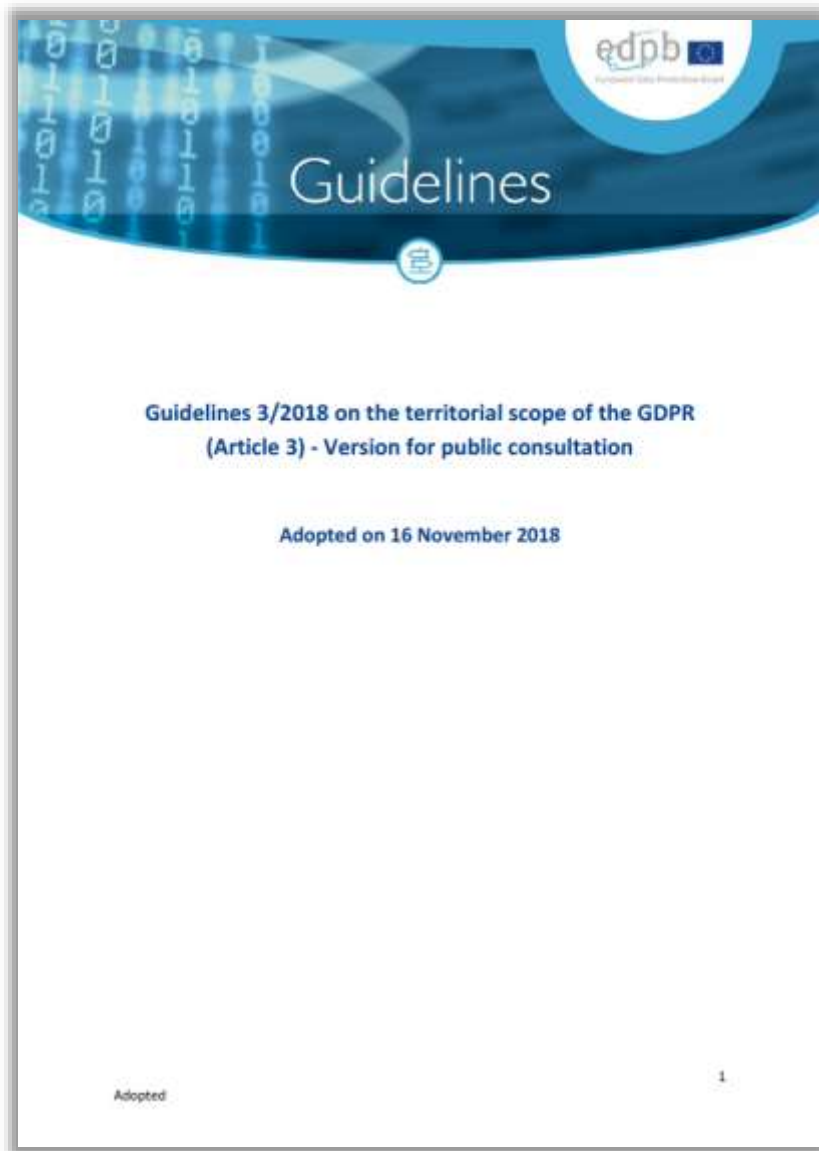
<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

<sup>4</sup> EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

<sup>5</sup> EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

**Сокращения:** ст. – статья, п. – пункт, гс. – пункт преамбулы (*recital*), exp. – пример (*example*).

## 522 Сфера действия GDPR: разъяснения EDPB

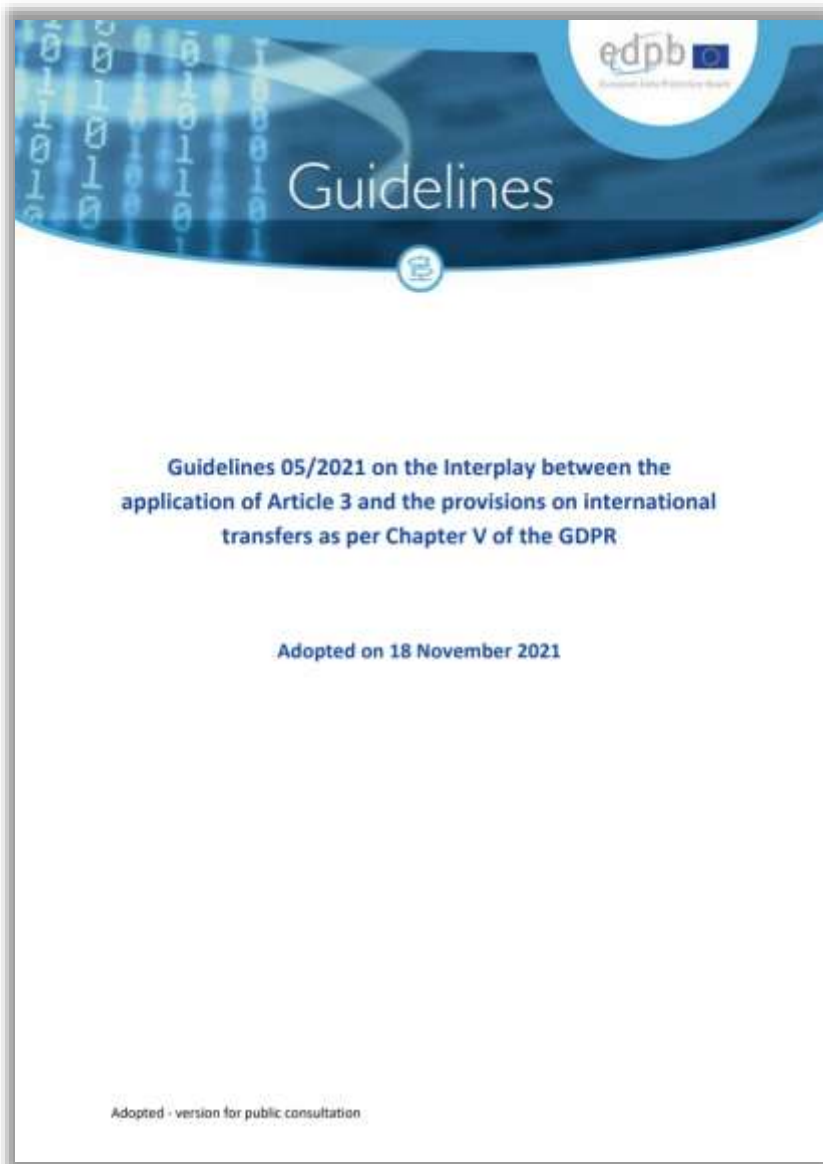


Европейский совет по защите данных (European Data Protection Board) на своем четвертом пленарном заседании 16.11.2018 принял проект разъяснений по определению территориального охвата GDPR, которые были опубликованы 23.11.2018 для проведения общественных консультаций. 12.11.2019 была опубликована итоговая версия разъяснений.

Эти разъяснения должны способствовать формированию общих подходов в толковании сферы применения требований GDPR и прояснению порядка применения требований GDPR в отношении контролеров данных или обработчиков данных, находящихся за пределами ЕС. В разъяснениях содержатся указания относительно трактовки требований о назначении представителя в ЕС.

При подготовке разъяснений использовался подготовленный Европейской комиссией «[Guide to the case law of the European Court of Justice on Articles 49 et seq. TFEU](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0650)».

## Взаимосвязь норм GDPR о его территориальном охвате и о международной передаче данных



Европейский совет по защите данных (European Data Protection Board) на своем пленарном заседании 19.11.2021 принял проект Руководящих принципов по взаимосвязи между применением норм о территориальном охвате GDPR (ст. 3) и положений главы V GDPR о международной передаче данных.

В документе указаны три совокупных критерия, которые квалифицируют обработку данных как трансграничную передачу:

1. экспортер данных (контроллер или процессор) подчиняется GDPR в отношении данной обработки;
2. экспортер данных передает или делает доступными персональные данные импортеру данных (другому контроллеру, совместному контроллеру или процессору);
3. импортер данных находится в третьей стране или является международной организацией.

Обработка данных будет считаться трансграничной передачей независимо от того, является ли импортер, находящийся в третьей стране, уже подпадающим под действие GDPR согласно ст.3. Однако сбор данных непосредственно от субъектов данных в ЕС по их собственной инициативе не является такой передачей.

**Обязательно назначение представителя в ЕС** для контролера или процессора, не осуществляющего в ЕС реальную деятельность через постоянную структуру, но предлагающего товары/услуги для ЕС или ведущего мониторинг поведения в ЕС.



**Исключения минимальны** – нерегулярная обработка данных, при которой:

1. Не обрабатываются большие объёмы специальных данных и данных о судимости и правонарушениях и
2. Маловероятны риски нарушения прав и свобод человека



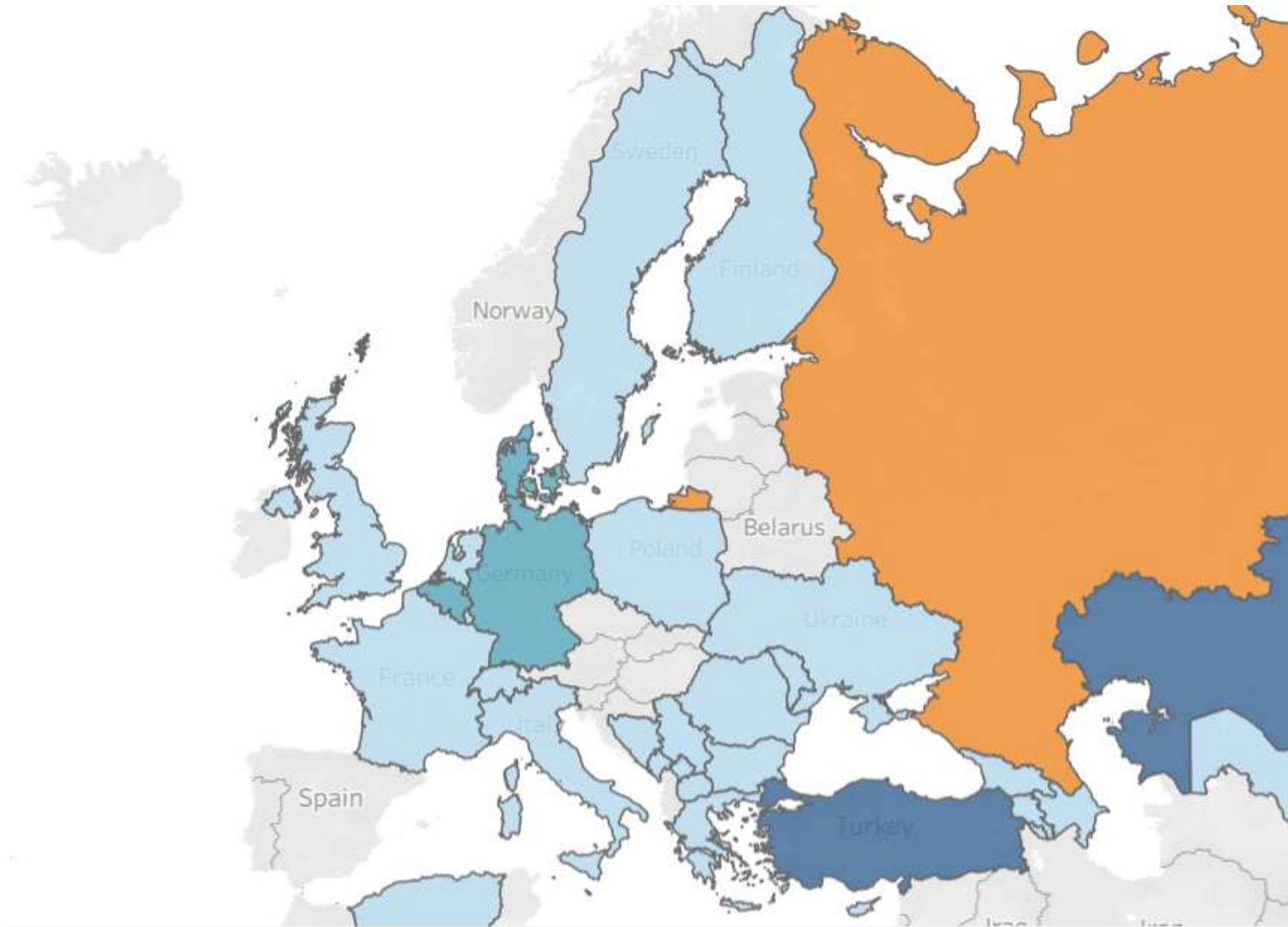
**Представитель в ЕС:**

1. Назначается в одной из стран ЕС, где данные обрабатываются
2. От имени контролера/процессора (вместо них или в дополнение) взаимодействует с властями ЕС и субъектами
3. Привлекается к ответственности за нарушения контролера/процессора

# Трансграничная обработка данных и Transfer Impact Assessment



526 Наличие требований по локализации обработки данных в ЕС/ЕЭЗ



Number of Regulations





**Некоторые из целей трансграничной передачи внутри транснациональной группы**

- ❖ заключение и (или) исполнение договоров и соглашений
- ❖ ведение деловых переговоров
- ❖ проявление должной осмотрительности
- ❖ участие в процедурах закупок
- ❖ осуществление информационного взаимодействия
- ❖ использование прав, исполнение обязанностей и соблюдение запретов, предусмотренных применимыми нормами

## Передача персональных данных при условии соблюдения соответствующих гарантий – статья 46(1-2) GDPR



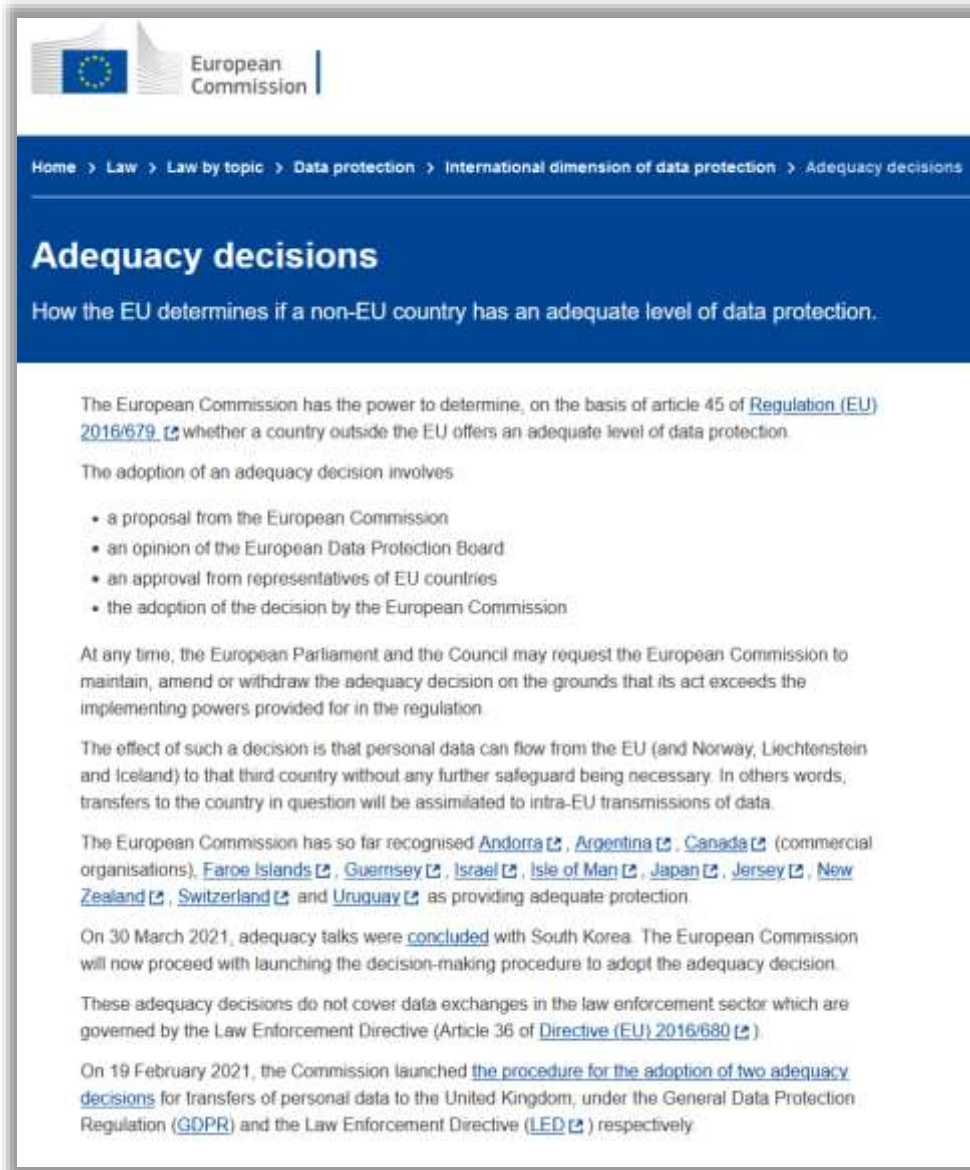
В случае отсутствия решения согласно Статье 45(3) контролер или обрабатывающее данные лицо могут передать персональные данные третьей стране или международной организации только, если контролер или обрабатывающее данные лицо предусмотрели соответствующие гарантии и если субъекты данных обладают юридически защищенными правами и эффективными средствами правовой защиты.

Соответствующие гарантии могут быть предоставлены без особого разрешения надзорного органа посредством:

- (a) имеющего обязательную юридическую силу документа между органами государственной власти или правительственными учреждениями;
- (b) юридически обязывающих корпоративных правил в соответствии со Статьей 47;
- (c) стандартных условий о защите данных, принятых Европейской Комиссией в соответствии с процедурой проверки, указанной в Статье 93(2);
- (d) стандартных условий о защите данных, принятых надзорным органом и утвержденных Европейской Комиссией согласно процедуре проверки, указанной в Статье 93(2);
- (e) утвержденной нормы поведения согласно Статье 40 совместно с юридически обязывающими и защищенными обязательствами контролера или обрабатывающего данные лица в третьей стране по применению соответствующих гарантий, в том числе в отношении прав субъектов данных; или
- (f) утвержденного сертификационного механизма согласно Статье 42 совместно с юридически обязывающими и защищенными обязательствами контролера или обрабатывающего данные лица в третьей стране по применению соответствующих гарантий, в том числе в отношении прав субъектов данных.



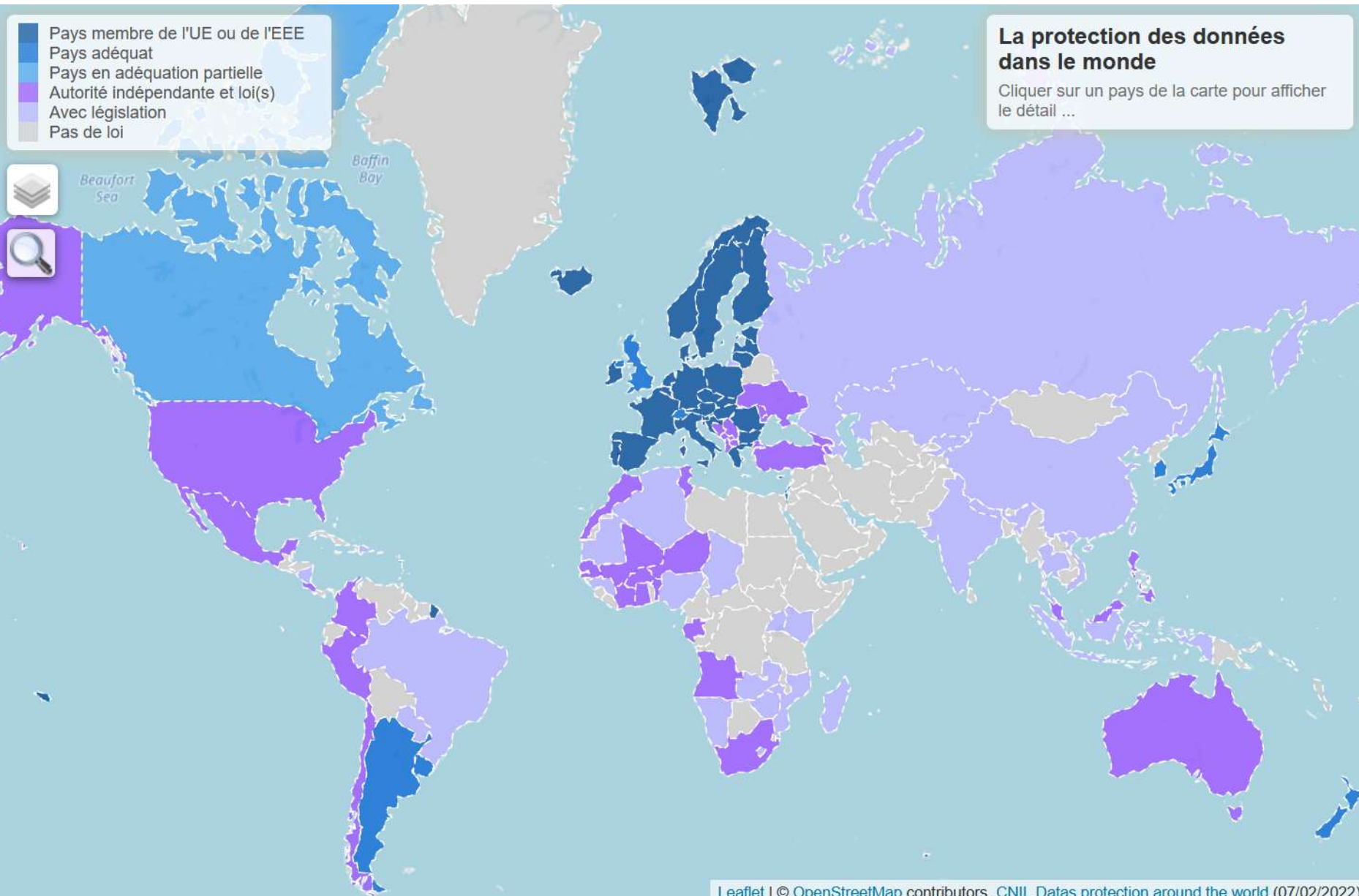
## Перечень стран, обеспечивающих адекватный уровень защиты данных согласно требованиям GDPR



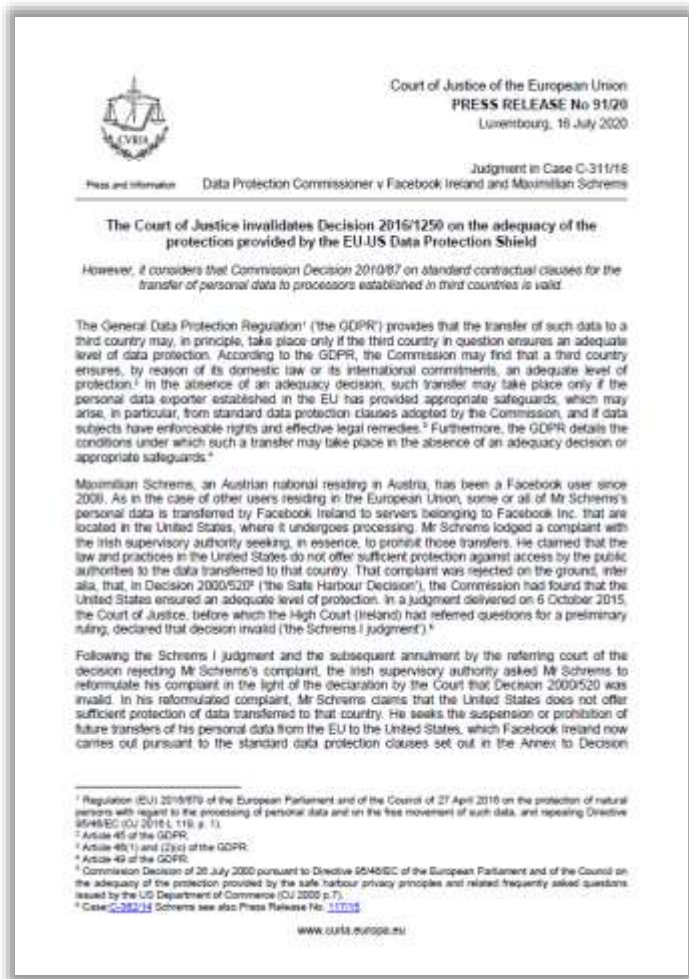
The screenshot shows the European Commission website page for 'Adequacy decisions'. The page header includes the European Commission logo and a navigation menu: Home > Law > Law by topic > Data protection > International dimension of data protection > Adequacy decisions. The main heading is 'Adequacy decisions' with a sub-heading 'How the EU determines if a non-EU country has an adequate level of data protection.' The text explains that the European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679, whether a country outside the EU offers an adequate level of data protection. It lists the steps for adopting an adequacy decision: a proposal from the European Commission, an opinion of the European Data Protection Board, an approval from representatives of EU countries, and the adoption of the decision by the European Commission. It also mentions that the European Parliament and the Council may request the Commission to maintain, amend, or withdraw the decision. The page lists countries recognized as providing adequate protection: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. It notes that on 30 March 2021, adequacy talks with South Korea were concluded, and the Commission will now proceed with the decision-making procedure. It also states that these decisions do not cover data exchanges in the law enforcement sector. Finally, it mentions that on 19 February 2021, the Commission launched the procedure for the adoption of two adequacy decisions for transfers of personal data to the United Kingdom, under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) respectively.

- [Andorra](#)
- [Argentina](#)
- [Canada](#) (коммерческие организации)
- [Faroe Islands](#)
- [Guernsey](#)
- [Israel](#)
- [Isle of Man](#)
- [Japan](#)
- [Jersey](#)
- [New Zealand](#)
- [South Korea](#)
- [Switzerland](#)
- [Uruguay](#)
- [United Kingdom](#)

## Европейский взгляд на обеспечение разными странами адекватного уровня защиты персональных данных



# CJEU о недействительности Privacy Shield и об уточнении в отношении стандартных договорных условий (SCC-P)



## Court of Justice of the European Union Judgment in Case C-673/17 Data Protection Commissioner v Facebook Ireland Limited, Maximilian Schrems

Суд постановил, что:

1. Privacy Shield признается недействительным в связи с недостаточной защищенностью персональных данных от передачи операторами социальных сетей американским спецслужбам. В решении суда говорится, что данное соглашение создает условия для нарушения фундаментальных прав европейских граждан. В нем подчеркивается, что в США доступ государственных структур к подобной информации ограничен в гораздо меньшей степени, чем в странах ЕС.

2. SCC-P (Standard Contractual Clauses Controller-to-Processor) не должны быть признаны недействительными, но экспортеры и импортеры персональных данных из ЕС должны предпринимать необходимые и достаточные меры для обеспечения соблюдения SCC-P. В частности, экспортер данных при содействии импортера должен оценить адекватность защиты прав субъектов данных в юрисдикции импортера данных, а также способен ли импортер данных выполнять все требования SCC-P. Кроме того, надзорные органы ЕС (DPA) обязаны приостановить или запретить передачу данных в третью страну, если они считают принципиально невозможным обеспечение требуемого законодательством ЕС уровня защиты прав субъектов данных, даже при наличии действующего SCC между экспортером и импортером.

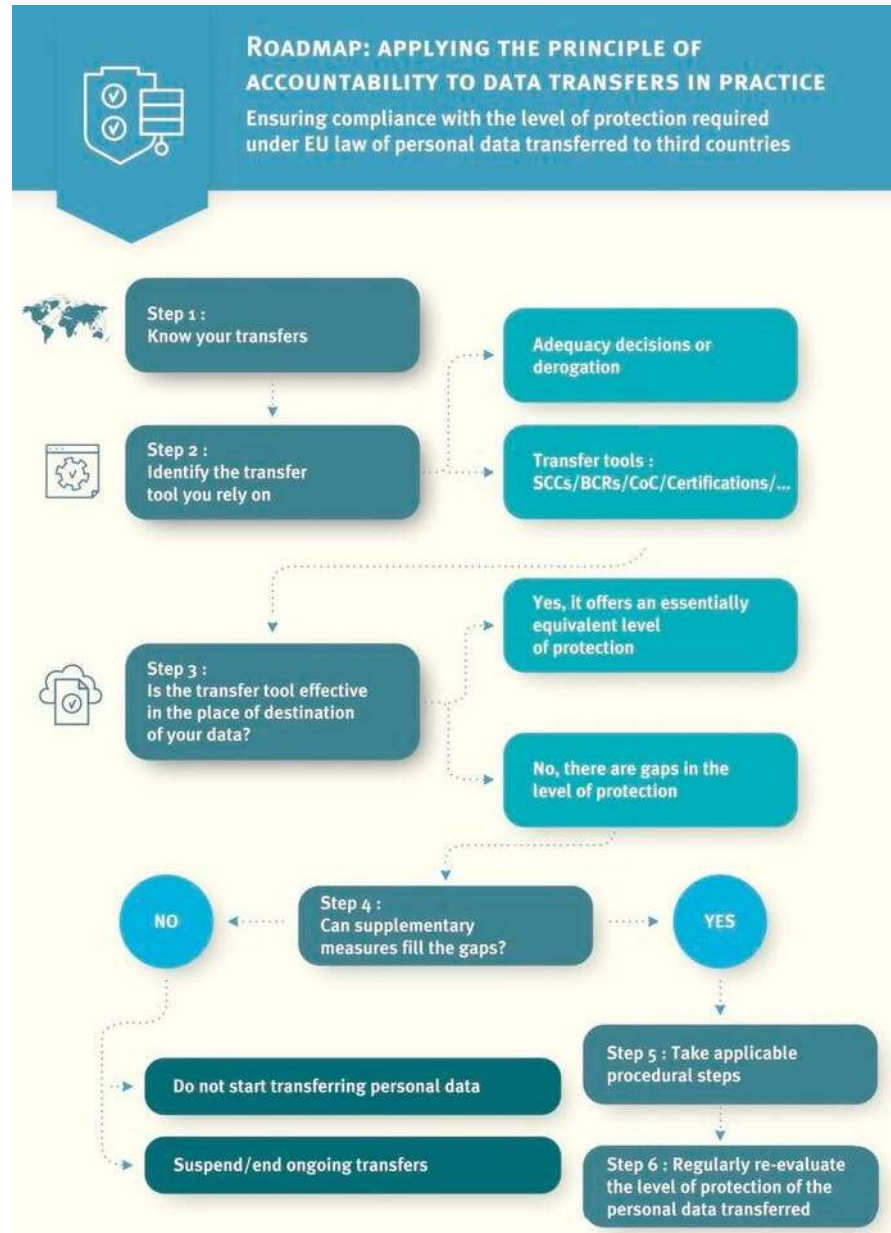
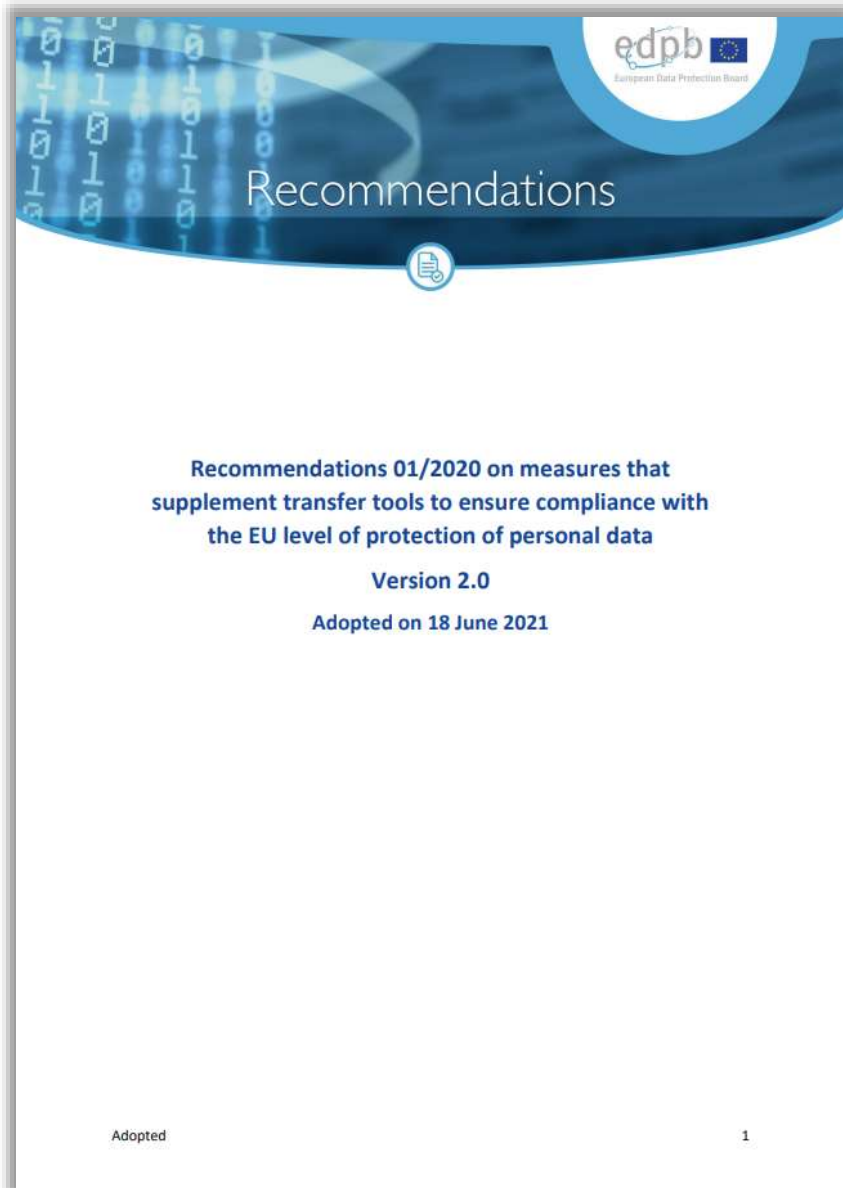
<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf>

История судебных разбирательств Schrems I и Schrems II <https://d-russia.ru/shrems-tretij-jepizod.html>

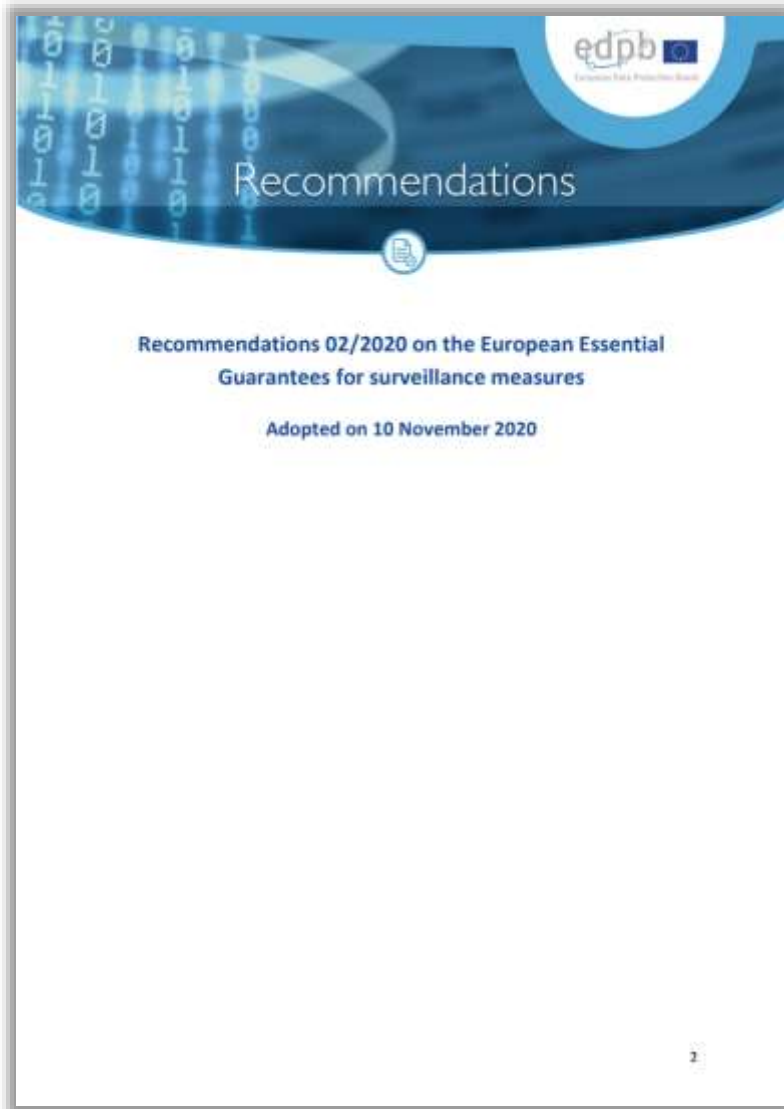
## Позиция EDPB по решению CJEU в рамках дела Schrems II: недействительность Privacy Shield и уточнение SCC-P

- EDPB поддерживает [решение CJEU от 16.07.2020 C-311/18 по делу Schrems II](#).
- Взамен признанного судом недействительным соглашения Privacy Shield ЕС и США должны создать эффективную систему, гарантирующую, что уровень защиты персональных данных, передаваемых в США, эквивалентен уровню защиты персональных данных в ЕС.
- Хотя SCC-P (Standard Contractual Clauses Controller-to-Processor) были признаны в качестве продолжающего действовать правового механизма для экспорта данных из ЕС, но экспортер и импортер данных должны совместно осуществить предварительную (до заключения SCC) оценку возможности обеспечения надлежащего уровня защиты прав субъектов данных в случае осуществления предполагаемой передачи данных. При проведении такой предварительной оценки экспортер (при необходимости, с помощью импортера) должен учитывать содержание SCC, специфику передачи данных, а также правовой режим, применимый в иностранной юрисдикции. Проверка последнего должна проводиться с учетом неисчерпывающих факторов, указанных в ст.45(2) GDPR.
- При выявлении такой необходимости по результатам предварительной оценки, экспортер данных должен рассмотреть возможность включения в SCC дополнительных положений, направленных на защиту прав субъектов данных.
- Если положения SCC в части гарантии прав субъектов данных не выполняются или не могут быть фактически выполнены в иностранной юрисдикции, то SCC обязывает экспортера приостановить передачу данных или расторгнуть SCC или проконсультироваться с компетентным надзорным органом ЕС по сложившейся ситуации, если экспортер намеревается продолжить передачу данных.
- Надзорные органы ЕС (DPA) обязаны приостановить или запретить передачу данных в третью страну на основании SCC между экспортером и импортером данных, если по мнению регулятора в юрисдикции третьей страны положения SCC не соблюдаются или не могут быть соблюдены.
- EDPB [подготовил FAQ](#) по использованию правовых механизмов для обеспечения правомерной передачи персональных данных в третьи страны с учетом решения суда. U.S. Department of Commerce также [подготовил FAQ](#) по обновлению программы EU-U.S. Privacy Shield.

# Рекомендации EDPB о дополнительных мерах обеспечения защиты персональных данных при трансграничной передаче




## Рекомендации EDPB о дополнительных гарантиях для субъектов при государственной слежке за ними



### Table of contents

1. INTRODUCTION .....	4
2. INTERFERENCES WITH FUNDAMENTAL RIGHTS .....	6
3. THE EUROPEAN ESSENTIAL GUARANTEES.....	8
Guarantee A - Processing should be based on clear, precise and accessible rules.....	8
Guarantee B - Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated .....	10
Guarantee C - Independent oversight mechanism.....	12
Guarantee D - Effective remedies need to be available to the individual .....	13
4. FINAL REMARKS .....	15



# Statement

## Statement 02/2022 on personal data transfers to the Russian Federation

Adopted on 12 July 2022

**The European Data Protection Board has adopted the following statement:**

Since 24 February 2022, the Russian Federation (Russia) is in a *de facto* state of war against Ukraine. As a consequence, it was excluded from the Council of Europe on 16 March 2022. Therefore, Russia is no longer a contracting party to those conventions and protocols concluded within the framework of the Council of Europe that are open only to its member States. It will also cease to be a High Contracting Party to the European Convention on Human Rights as of 16 September 2022.

While, in its decision adopted on 23 March 2022, the Committee of Ministers of the Council of Europe stated that Russia will continue to be a contracting party to those conventions and protocols concluded in the framework of the Council of Europe to which it has expressed its consent to be bound and which are open to accession by non-member States – for instance, Convention 108 –, the modalities of Russia's participation in these instruments are still to be determined<sup>2</sup>. Such changes could have a significant impact on the level of protection of data subjects.

The European Data Protection Board (EDPB) recalls that the transfer of personal data to a third country, in the absence of an adequacy decision of the European Commission pursuant to Article 45 GDPR, is only possible if the controller or processor has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies are available for data subjects (Article 46 GDPR). In the absence of an adequacy decision pursuant to Article 45(3) GDPR, or of appropriate safeguards pursuant to Article 46 GDPR, a transfer or a set of transfers of personal data to a third

Adopted

country shall take place, in specific circumstances, only on one of the conditions set forth in Article 49 GDPR ("Derogations for specific situations")<sup>3</sup>.

Russia does not benefit from an adequacy finding by the European Commission in accordance with Article 45 GDPR. Therefore, transfers of personal data to Russia must be carried out using one of the other transfer instruments provided for in Chapter V GDPR. Having this in mind, the EDPB notes that, when personal data are transferred to Russia, data exporters under the GDPR should assess and identify the legal basis for the transfer and the instrument to be used among those provided by Chapter V GDPR (e.g., Standard Contractual Clauses or Binding Corporate Rules), in order to ensure the application of appropriate safeguards.

Furthermore, the EDPB recalls that, following the *Schrems II* ruling of the European Court of Justice<sup>4</sup>, and according to the EDPB Recommendations on supplementary measures<sup>5</sup>, data exporters should assess if, in the context of the transfer at stake, there is anything in the law and/or practices in force in Russia (in particular, regarding access to personal data by the Russian public authorities, especially for criminal law enforcement and national security purposes) that may impinge on the effectiveness of the appropriate safeguards provided by the transfer instruments identified. If this is the case, data exporters should identify and adopt supplementary measures that are necessary to ensure that data subjects are afforded a level of protection that is essentially equivalent to that guaranteed within the EEA<sup>6</sup>. Where such assessment leads to the conclusion that compliance is not (or no longer) ensured, and that no supplementary measures could be identified, data exporters have to suspend data transfers.

Several Member States of the EEA have close economic and historic ties with Russia, therefore frequent exchanges of personal data occur between these countries and Russia. Some national data protection supervisory authorities are already looking into the lawfulness of data transfers to Russia, including in the context of ongoing investigations. Supervisory authorities will continue to monitor legislative changes and other relevant developments in Russia that could have an impact on data transfers. They will handle cases involving data transfers to Russia taking into account the increased impact on the rights and freedoms of data subjects that may arise from such data processing operations, and will coordinate within the EDPB, as appropriate.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

---

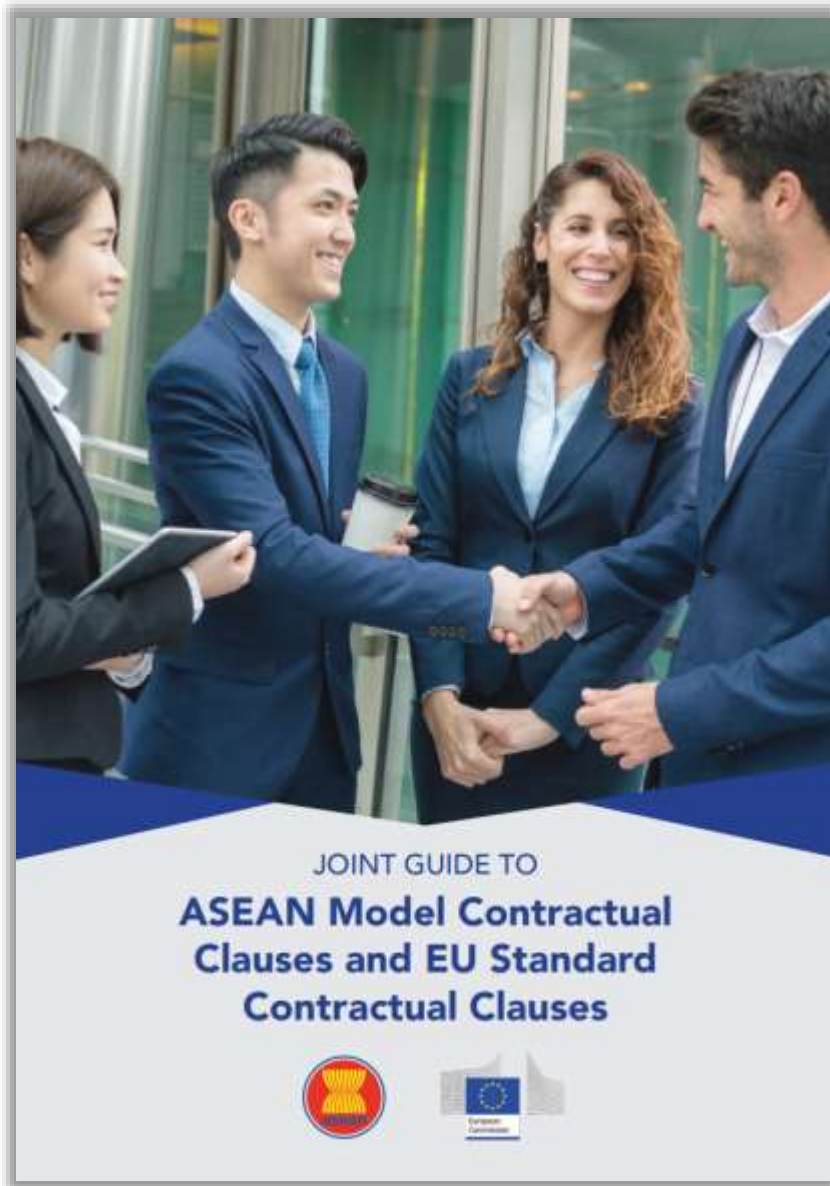
<sup>1</sup> See Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, available at [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-2018-derogations-article-49-under-regulation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-2018-derogations-article-49-under-regulation_en).

<sup>2</sup> CJEU, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECU EU:C:2020:559.

<sup>3</sup> EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, final version adopted on 18 June 2021, available at [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer\\_en](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en).

<sup>4</sup> The European Economic Area, abbreviated as EEA, consists of the Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway, excluding Switzerland).

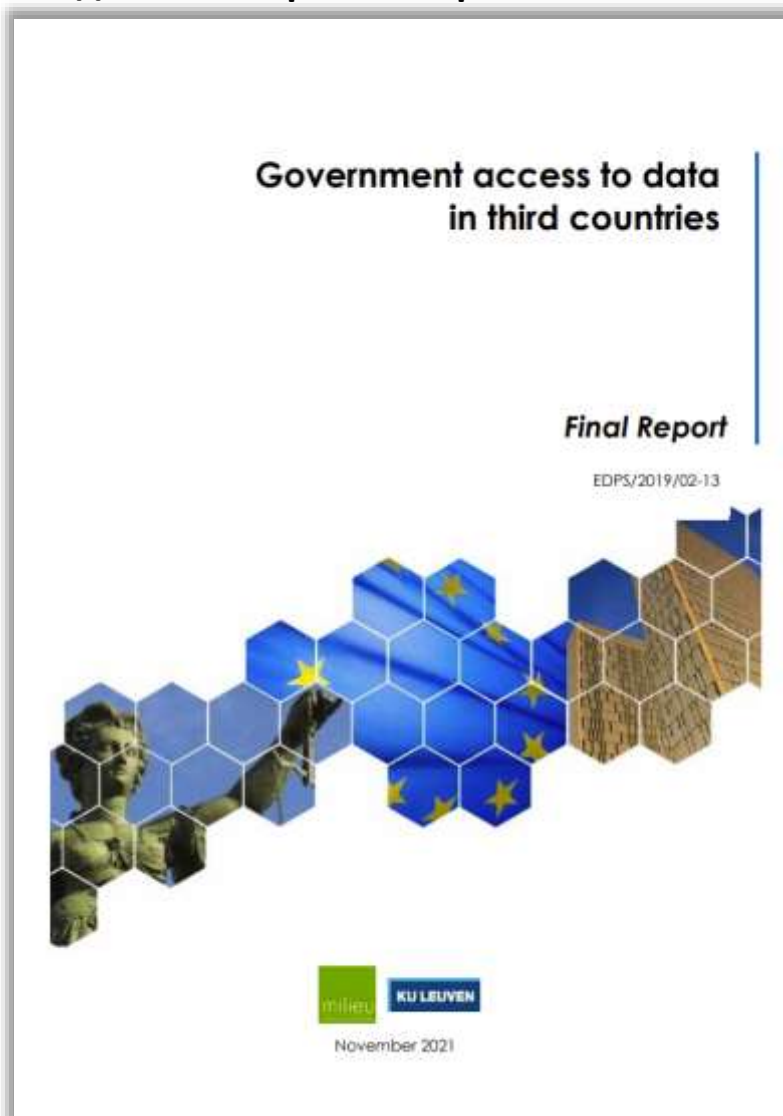
## ЕС и АСЕАН выпустили руководство по стандартным договорным положениям для передачи данных



◇ 24.05.2023 ЕС и Ассоциация государств Юго-Восточной Азии (АСЕАН) выпустили совместное руководство, в котором определены общие черты между стандартными договорными положениями ЕС (SCCs) и типовыми договорными положениями АСЕАН для трансграничных потоков данных (MCCs). Цель руководства - помочь компаниям, работающим в двух регионах, как экспортерам, так и импортерам данных, понять сходства и различия между SCCs и MCCs, чтобы облегчить соблюдение ими соответствующих требований по защите данных.

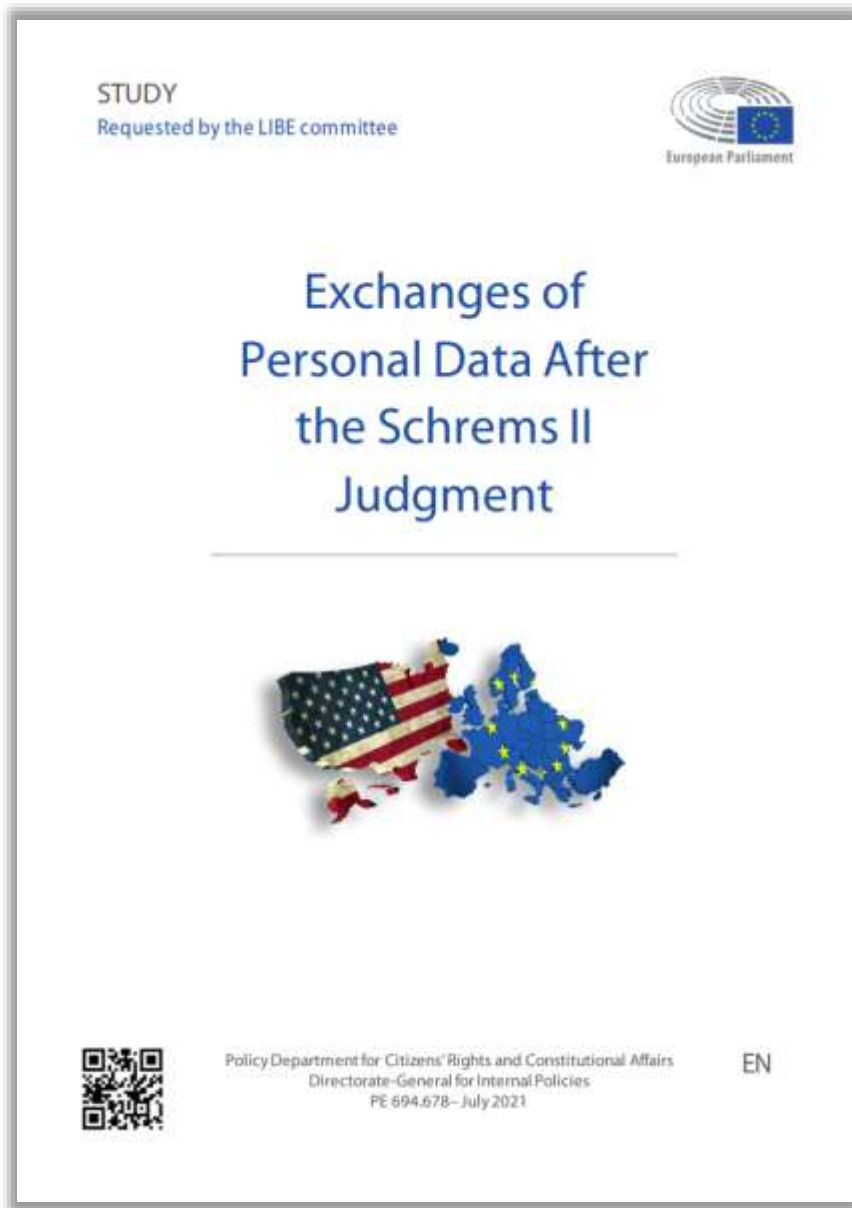
◇ Руководство также охватывает как обязательства по передаче данных от контроллера к контроллеру, так и обязательства по передаче данных от контроллера к процессору. Отдельно в руководстве указано, что оно представляет собой первую часть серии из двух частей, и что во второй части будут представлены лучшие практики компаний, которые используют как SCCs, так и MCCs для передачи данных.





<b>EXECUTIVE SUMMARY</b> .....	<b>4</b>
<b>1 INTRODUCTION</b> .....	<b>6</b>
1.1 Objectives and scope of the study .....	6
1.2 Legal background.....	6
1.2.1 Legality .....	7
1.2.2 Objectives of general interest .....	8
1.2.3 Proportionality.....	8
1.3 Study methodology.....	9
1.4 Structure of this report.....	10
<b>2 IN-DEPTH ANALYSIS OF THIRD COUNTRIES</b> .....	<b>12</b>
2.1 China.....	12
2.1.1 Rule of law, respect for human rights and fundamental freedoms	12
2.1.2 Government access to personal data .....	15
2.1.3 Data subject rights and redress mechanisms .....	19
2.1.4 Are the new laws on data protection in the PRC a game-changer for government access?.....	22
2.1.5 Intermediary conclusion.....	24
2.2 India.....	26
2.2.1 Rule of law, respect for human rights and fundamental freedoms	26
2.2.2 Government access to personal data .....	28
2.2.3 Data subject rights .....	35
2.2.4 Upcoming changes in legislation .....	38
2.2.5 Intermediary conclusion.....	38
2.3 Russia.....	40
2.3.1 Rule of law, respect for human rights and fundamental freedoms	40
2.3.2 Government access to personal data .....	45
2.3.3 Data subject rights .....	50
2.3.4 Upcoming changes in legislation .....	52
2.3.5 Intermediary conclusion.....	52
<b>3 CONCLUSION</b> .....	<b>55</b>
<b>ANNEX 1 – QUESTIONNAIRES</b> .....	<b>57</b>
<b>ANNEX 2 – SOURCES OF INFORMATION</b> .....	<b>63</b>
<b>ANNEX 3 - ACRONYMS AND ABBREVIATIONS</b> .....	<b>70</b>

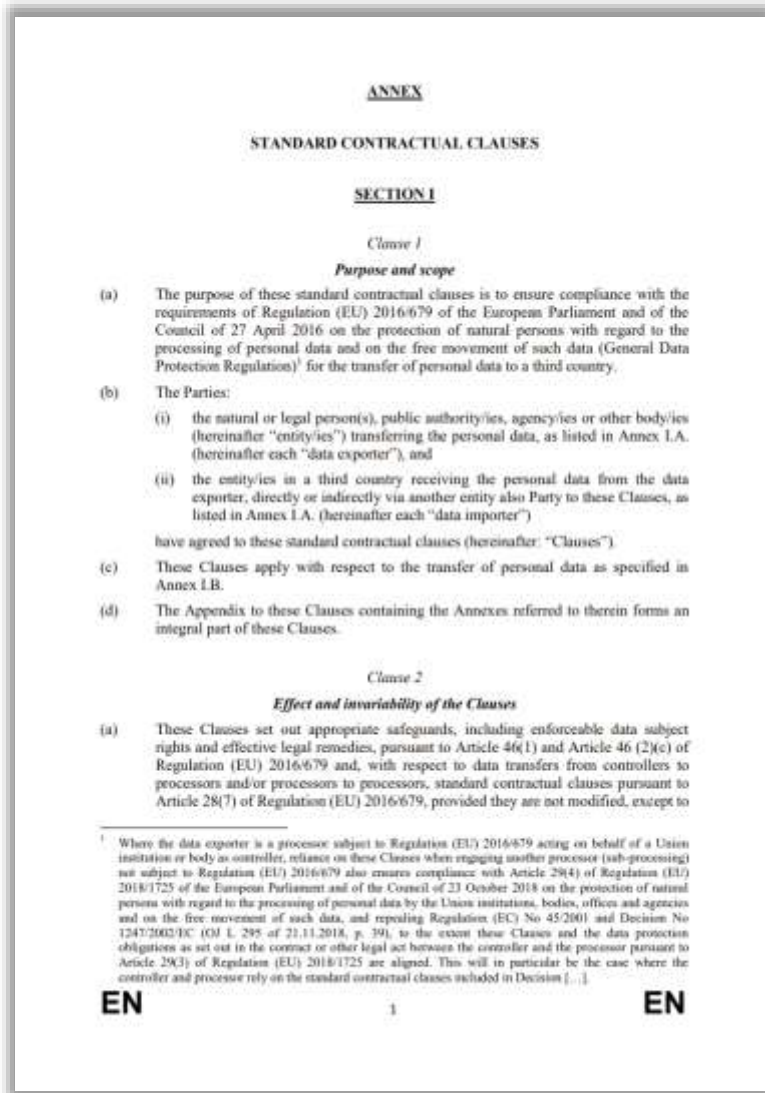
## Трансграничный обмен персональными данными между ЕС и США после решения Schrems II



В этом исследовании, проведенном по заказу Департамента политики по правам граждан и конституционным вопросам Европейского парламента по запросу Комитета LIBE, рассматриваются вопросы реформы европейского регулирования в соответствии с постановлением Суда ЕС по Schrems II относительно обмена персональными и другими данными между ЕС и США.

Авторы исследования:

- Ian BROWN, Visiting CyberBRICS professor at Fundação Getulio Vargas (FGV) Law School in Rio de Janeiro, Brazil
- Douwe KORFF, Emeritus Professor of International Law, London Metropolitan University, UK



04.06.2021 Европейская Комиссия опубликовала новые Стандартные договорные условия для экспорта персональных данных из ЕС/ЕЭЗ в иностранные государства, не обеспечивающие адекватную защиту прав субъектов данных. Также было предложено, спустя 18 месяцев после утверждения новых SCC, признать не имеющими силу ранее принятые SCC-C и SCC-P.

Новые SCC использует модернизированный подход:

1. модульность SCC, описывающие различные сценарии передачи данных в одном документе, чтобы стороны могли адаптировать свои договоры к уникальному контексту их цепочек передачи и обработки;
2. всего предусмотрено 4 сценария передачи данных:
  - от контролера к контролеру;
  - от контролера к процессору;
  - от процессора к процессору;
  - от процессора к контролеру.
3. SCC могут быть не только двусторонними, но и многосторонними, в т.ч. подразумевают возможность режима «договор присоединения».

## THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS

### OVERVIEW

INTRODUCTION .....	4
<b>I. STANDARD CONTRACTUAL CLAUSES .....</b>	<b>4</b>
<b>GENERAL.....</b>	<b>4</b>
1. What are Standard Contractual Clauses? .....	4
2. Which Standard Contractual Clauses have been adopted by the European Commission? ...	4
3. What are the advantages of using SCCs?.....	5
4. What was the process followed by the European Commission in developing the SCCs? .....	5
5. Will the European Commission evaluate after some time how the new SCCs work in practice?.....	5
<b>SIGNATURE, MODIFICATIONS AND RELATIONSHIP WITH OTHER CONTRACTUAL PROVISIONS.....</b>	<b>6</b>
6. Are there specific requirements for the signature of the SCCs by the parties? .....	6
7. Can the text of the SCCs be changed? .....	6
8. Is it possible to add additional clauses to the SCCs or incorporate the SCCs into a broader commercial contract? .....	6
9. Can the parties delete modules and/or options that do not apply to their situation? .....	7
10. How should the SCCs be incorporated into a commercial contract? .....	7
<b>CHANGES TO THE PARTIES .....</b>	<b>8</b>
11. What is the purpose of the so-called ‘docking clause’?.....	8
12. How does the docking clause work in practice? Are there any formal requirements for allowing new parties to accede?.....	8
13. What happens when a new party accedes to the SCCs? Are there any formalities to take care of? .....	8
<b>II. STANDARD CONTRACTUAL CLAUSES BETWEEN CONTROLLERS AND PROCESSORS .....</b>	<b>9</b>
14. What is the difference between SCCs adopted by national data protection authorities and the SCCs adopted by the Commission? .....	9
15. In which form should instructions by the controller be given to the processor?.....	9
16. Is the processor required to provide the name(s) of the sub-processor(s) it engages to the controller? .....	9
17. What happens if the controller objects to changes of sub-processors, in case a general authorisation to the engagement of sub-processors was given?.....	9

18. What is the required time period for the processor to notify the controller of a data breach? .....	9
19. Besides a review or an audit, can the processor demonstrate compliance with its requirements under the SCCs by other means?.....	10

### III. STANDARD CONTRACTUAL CLAUSES FOR DATA TRANSFERS TO THIRD COUNTRIES..... 11

#### REASONS FOR MODERNISATION AND MAIN NOVELTIES .....

20. Why did the Commission modernise the previous SCCs for international data transfers? .....	11
21. What are the main novelties compared to the previous SCCs? .....	11
22. Are data exporters and importers that still use the “old” SCCs (adopted under the 1995 Data Protection Directive) required to switch to the new ones (adopted in 2021)? .....	12

#### SCOPE OF APPLICATION AND TRANSFER SCENARIOS .....

23. For which transfers can the SCCs be used? .....	13
24. Can these SCCs be used for data transfers to controllers or processors whose processing operations are directly subject to the GDPR?.....	13
25. Can the SCCs be used to transfer personal data to an international organisation?.....	14
26. Can the SCCs only be used for international data transfers under the GDPR? .....	14
27. What are the different ‘modules’ and how should the right one be chosen? .....	14
28. Can several modules be agreed between the same parties at the same time?.....	15
29. How can compliance with Article 28 of the GDPR be ensured when transferring data to a processor or a sub-processor outside of the EEA? .....	15
30. In which scenarios should Module 4 (processor to controller) be used?.....	16

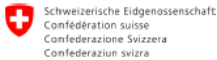
#### INDIVIDUALS: YOUR RIGHTS WHEN YOUR DATA IS TRANSFERRED BASED ON THE SCCs 16

31. How can I know that my data is transferred outside of Europe based on the SCCs?.....	16
32. I have been informed that my data has been transferred outside the EEA based on SCCs. How can I obtain more information about the actual transfers, my rights as a data subject and the applicable safeguards? Can I obtain a copy of the SCCs?.....	16
33. What if my data was processed in violation of the SCCs, can I obtain redress (e.g. compensation for damages)? Where can I lodge a complaint? .....	17

#### OBLIGATIONS OF DATA EXPORTERS AND IMPORTERS .....

34. For Modules 1, 2 and 3: does the data importer have to take specific steps when sharing personal data it has received with third parties? .....	18
35. Can liability under the SCCs be limited by general liability clauses in the main services/commercial agreement?.....	19

## FDPIС признал недостаточный уровень защиты конфиденциальности данных в Swiss-US Privacy Shield



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Federal Data Protection and Information Commissioner FDPIС

Policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 Para. 1 Swiss Federal Act on Data Protection

### 1. Significance and impact of the Federal Data Protection and Information Commissioner (FDPIС) list of countries

In accordance with Art. 7 OFADP,<sup>1</sup> the FDPIС maintains a list of countries documenting the adequacy of data protection in these countries within the meaning of Art. 6 FADP.<sup>2</sup> This list is publicly available.

In maintaining the list, the FDPIС takes the following into consideration:

- Legislation and its practical application by the individual countries and how this legislation is assessed by academia and courts;
- Conventions, publications, official statements and decisions by domestic and foreign institutions and authorities on the equivalence or adequacy of the level of data protection afforded by other countries or international organisations.

As a result of a large number of country decisions on the adequacy of data protection, Switzerland, together with the countries of the European Union (EU), the European Economic Area (EEA), and some non-European countries such as Argentina, Canada, New Zealand and Uruguay, now belongs to a group of nations which mutually assume the existence of an equivalent and adequate level of data protection.<sup>3</sup> This means that, generally, personal data can be transferred between Switzerland and other countries in the group without any special safeguards within the meaning of Art. 6 Para. 2 FADP, as it is the case for data transfers in a domestic context.

When these countries assess the adequacy of another country's data protection levels, its data protection legislation is considered as a whole, including the requirements which apply when personal data exchanged between the countries concerned is exported to a third country. There is thus a shared expectation between these countries – i.e. also between Switzerland and the EU and EEA member states – that the list of countries will be kept updated in such a way that the level of protection considered mutually adequate will be respected at all times. A mutual need for coordination arises in particular when the adequacy of a third country has been reassessed, as it is currently the case in the EU/EEA member states<sup>4</sup> following the latest ruling by the Court of Justice of the European Union (CJEU) with regard to the USA.

<sup>1</sup> Ordinance of 14 June 1993 to the Federal Act on Data Protection, SR 235.11

<sup>2</sup> Federal Act of 19 June 1992 on Data Protection, SR 235.1

<sup>3</sup> Cf. in particular decisions by the European Commission in application of Art. 25 of the Directive and also Section 2.3.3 of the FOJ explanations on the revision of the Ordinance to the Federal Act of 14 June 1993 on Data Protection: explanations on the draft of 18 January 2007, which still refer to Directive 95/48/EC of 24 October 1995.

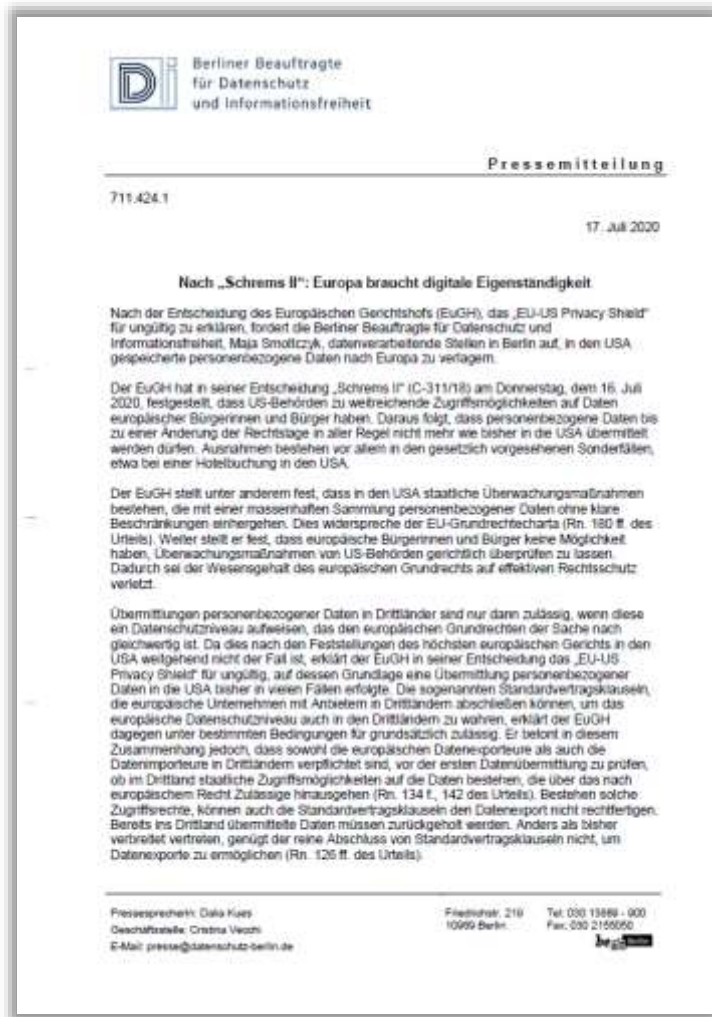
<sup>4</sup> The repeal of the adequacy finding is directly applicable in the EEA-EFTA countries.

Fedeggweg 1, 3003 Bern  
Tel. 058 463 74 84, Fax 058 465 99 96  
www.edoeb.admin.ch

Швейцарский Федеральный комиссар по защите данных и информации (FDPIС) 2020.09.08 объявил, что Соглашение о защите конфиденциальности данных между Швейцарией и США (Swiss-US Privacy Shield) не гарантирует адекватный уровень защиты при передаче данных из Швейцарии в США.

Поскольку Швейцария и ЕС взаимно признают свое законодательство о защите данных как эквивалентное, FDPIС соглашается с критикой EDPB относительно доступа властей США к данным. Более того, FDPIС указал, что некоторые принципы, закрепленные в Федеральном законе о защите данных (FADP), не соблюдаются в рамках Соглашения о защите конфиденциальности Швейцарии и США, включая законную обработку персональных данных и право на обращение в суд.

FDPIС указал, что его оценка Swiss-US Privacy Shield зависит от решений швейцарских судов и не влияет на существование Программы Privacy Shield и что она может использоваться заинтересованными лицами в Швейцарии до тех пор, пока не будет отменена США.



Берлинский надзорный орган (Berliner Beauftragte für den Datenschutz und die Informationsfreiheit) на основании решения CJUE по делу Schrems II указал экспортерам данных на то, что они не могут передавать персональные данные в иные юрисдикции при наличии у иностранного государства и иных лиц прав доступа к данным резидентов ЕС в большем объеме, чем это предусмотрено законодательством ЕС. Надзорный орган также попросил всех контролеров данных уважать решение CJEU и прекратить использовать облачные сервисы обработки данных (в частности, SaaS), провайдеры которых расположены в США. Вместо этого контролеры должны отдать предпочтение облачным сервисам, провайдеры которых расположены в ЕС или иных странах, обеспечивающих адекватный уровень защиты прав субъектов.

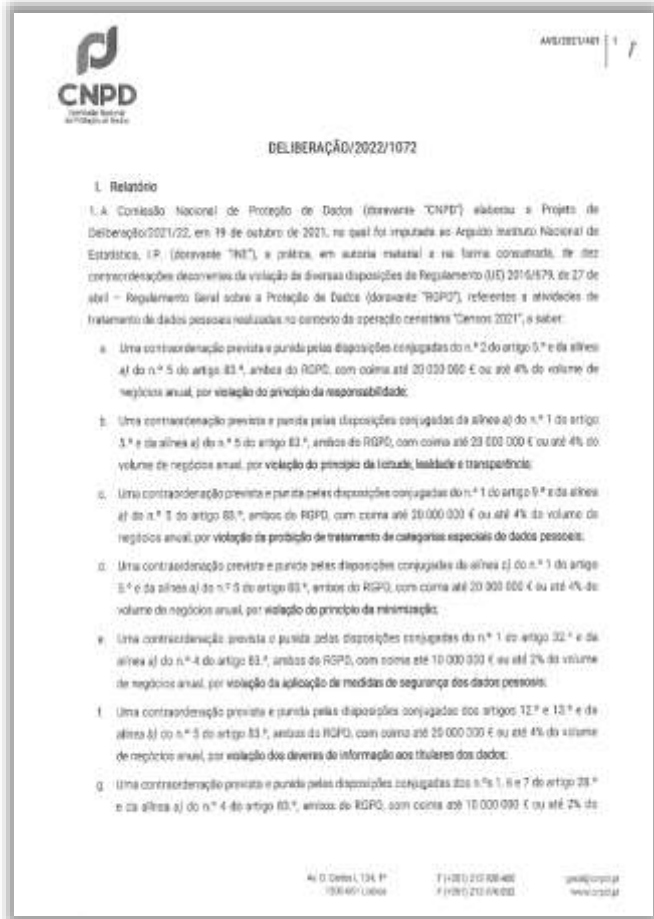
## Португальский надзорный орган запретил трансграничную передачу данных в адрес компании Cloudflare



27.04.2021 португальский орган по защите данных (CNPD) издал предписание, требующее от Национального статистического института (INE) приостановить в течение 12 часов любую трансграничную передачу персональных данных, в частности данных переписи 2021 года, в США или другие третьи страны без адекватного уровня защиты в соответствии с решением CJEU Schrems II. В решении отмечается, что после жалоб на условия сбора данных для переписи 2021 года CNPD провела расследование и пришла к выводу, что INE привлекла компанию Cloudflare, Inc. в качестве сервис-провайдера обработки данных.

Cloudflare является калифорнийской компанией и напрямую подчиняется законодательству США о слежке в целях обеспечения национальной безопасности, которое налагает юридическое обязательство предоставлять властям США неограниченный доступ к любым данным, находящимся во распоряжении компании, без права уведомления о таком доступе других лиц (субъектов данных).

Регулятор также отметил, что передаваемые данные включали такие чувствительные категории как сведения о религиозных убеждениях и о состоянии здоровья. Поэтому CNPD принял решение, что передача таких данных в США или любую другую третью страну без надлежащей защиты должна быть приостановлена.



**Кто:** Comissão Nacional de Protecção de Dados (Португалия)

**Кого:** Национальный институт статистики

**Когда:** 2022.12

**За что:** нарушение ст. 9(1), 12, 13, 28(1), 28(6), 28(7), 35(1), 35(2), 35(3)(b), 44, 46(2) GDPR

**Как:** штраф €4,300,000

**Причина:** Национальный институт, обрабатывая специальные данные, касающиеся здоровья и религии, не предоставил четкой и полной информации о необязательном характере их предоставления гражданами и не объяснил в достаточной мере, что некоторые из вопросов являются необязательными, тем самым не дав гражданам возможности сформировать свою волю, что является необходимым для предположений о законности обработки этих специальных категорий данных.

Кроме того, контролер заключил договор с компанией Cloudflare, Inc., базирующейся в США, на обработку данных в любом из 200 серверов Cloudflare, при этом обе компании предполагали, что данные могут обрабатываться за пределами ЕЭЗ. Хотя договор также включал в себя SCC для передачи персональных данных в США, но не предусматривал никаких дополнительных мер безопасности, как того требует решение CJEU по делу Schrems II. Национальный институт не проводил никакой оценки воздействия на защиту данных ("DPIA"), связанной с обработкой.



## Баварский надзорный орган запретил трансграничную передачу данных в адрес компании Mailchimp



edpb  
European Data Protection Board

≡ MENU

### Bavarian DPA (BayLDA) calls for German company to cease the use of 'Mailchimp' tool

Tuesday, 30 March, 2021 DE

The "ruling" presented in the "Standard" concerns a remedy procedure concluded without formal supervisory measures regarding a complaint by a data subject, in which the controller (an individual company) that had used Mailchimp had, after our request for comments and detailed information on the consequences of the Schrems II- decision, announced that it had now refrained from using Mailchimp.

Our final notice to the complainant, which apparently formed the basis of the publication and was sent in mid-March, had the following wording in extracts and translated informally:

*"... We are referring to your data protection complaint against ... concerning the use of "Mailchimp". As a result of our intervention, the company has informed us that it had used Mailchimp twice to send newsletters. As a result of our intervention, the company has now informed us that it will no longer use Mailchimp with immediate effect.*

*The company also informed us that it had only transmitted email addresses to Mailchimp in the context of the above-mentioned use. It also mentioned that the recommendations of the European Data Protection Board on the so-called Supplementary Measures for transfers of personal data to third countries are not yet available in a final version, but are still*

15.03.2021 баварское DPA завершило расследование по жалобе на неназванную немецкую компанию, которая дважды использовала американскую платформу электронного маркетинга Mailchimp для информационной рассылки своим клиентам. Хотя компания предоставила Mailchimp адреса электронной почты в соответствии с SCC, DPA Баварии сочло передачу незаконной, поскольку компания не проверила, потребуются ли «дополнительные меры» в соответствии с решением CJEU Schrems II для обеспечения адекватной защиты данных.

Баварский надзорный орган принял свое решение исходя из наличия «признаков того, что Mailchimp в принципе может получать запросы на доступ к данным со стороны американских спецслужб», и, следовательно, трансграничная передача данных из ЕС может быть дозволена только при условии принятия экспортёром и импортёром данных дополнительных мер защиты, которые будут достаточными для устранения потенциальной угрозы неправомерного доступа к данным. В конце концов, расследование было прекращено по причине прекращения использования сервиса Mailchimp со стороны немецкой компании.

[https://edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool\\_en](https://edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool_en)

<https://www.project-disco.org/european-union/040621-the-monkeys-pause-mailchimp-data-transfers-halted-in-german-schrems-ii-inquiry/>

## Австрийский DSB решил, что использование Google Analytics нарушает решение CJEU "Schrems II"



13.01.2022 австрийский орган по защите данных («Datenschutzbehörde» или «DSB») принял новаторское решение по жалобе австрийской НКО NOYB о том, что постоянное использование Google Analytics нарушает GDPR. Это первое решение по 101 типовой жалобе, поданной NOYB после так называемого решения «Шремс II». В 2020 году Суд (CJEU) постановил, что использование американских провайдеров нарушает GDPR, поскольку законы США о слежке требуют, чтобы американские провайдеры, такие как Google или Facebook, предоставляли личные данные властям США. Аналогичные решения ожидаются и в других странах-членах ЕС.

## Австрийский DSB: сервис Google по анонимизации IP-адресов и риск-ориентированный подход нарушают решение CJEU "Schrems II"



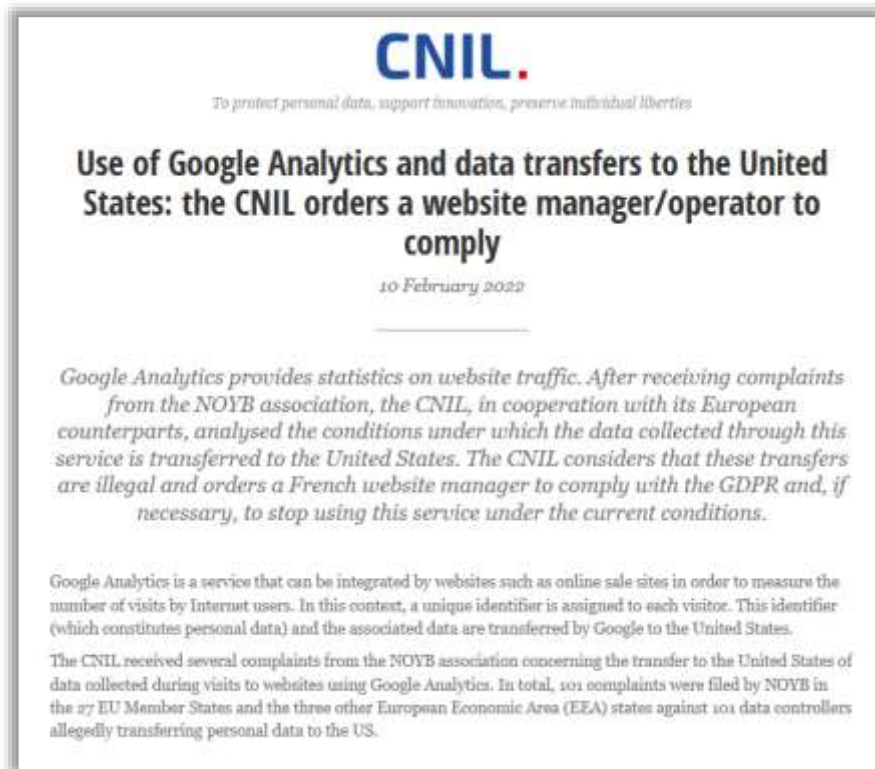
22.04.2022 австрийский орган по защите данных («Datenschutzbehörde» или «DSB») принял решение о том, что использование сервиса Google по анонимизации IP-адресов и риск-ориентированный подход в отношении трансграничной передачи данных в США не могут быть применены для обхода решения CJEU "Schrems II".

В настоящее время в ЕС активно продвигается риск-ориентированный подход, согласно которому обеспечение дополнительных гарантий для субъектов данных из ЕС требуется только в случае наличия «существенного риска для прав и свобод субъекта данных». По мнению некоторых прайваси-экспертов, стандартных договорных положений (SCC) будет достаточно для «случаев с низким уровнем риска», например, когда передаются такие данные как онлайн-идентификаторы или IP-адреса. DSB считает, что эта точка зрения неверна: GDPR не знает риск-ориентированного подхода к передаче данных в небезопасные третьи страны, такие как США.

DSB также отверг аргументы Google о том, что владельцы Интернет-ресурсов могут активировать сервис анонимизации IP-адресов пользователей, фиксируемых при помощи Google Analytics, для эффективной защиты конфиденциальности передаваемых в Google данных. Причины две:

- сервис анонимизации применяется только к IP-адресам, но онлайн-идентификаторы cookie или данные пользовательских устройств передаются в открытом виде;
- анонимизация IP-адресов происходит только **после** передачи данных в Google.

## Французский CNIL решил, что использование Google Analytics нарушает решение CJEU "Schrems II"



Французская национальная комиссия по информатике и свободам (Commission Nationale de l'Informatique et des Libertés, CNIL) рассмотрела поступившие жалобы на американский сервис Google Analytics. Изучение трафика показало, что Google Analytics собирает персональные данные граждан Франции и отправляет их на американские серверы в нарушение европейских законов GDPR.

10.02.2022 CNIL запретила использовать эту систему веб-аналитики в нынешнем виде. Официальное решение обязательно для исполнения операторами всех веб-сайтов Франции. На выполнение требований есть месяц.

Из текста официального решения можно сделать вывод, что CNIL признала персональными данными численный идентификатор пользователя (Client ID):

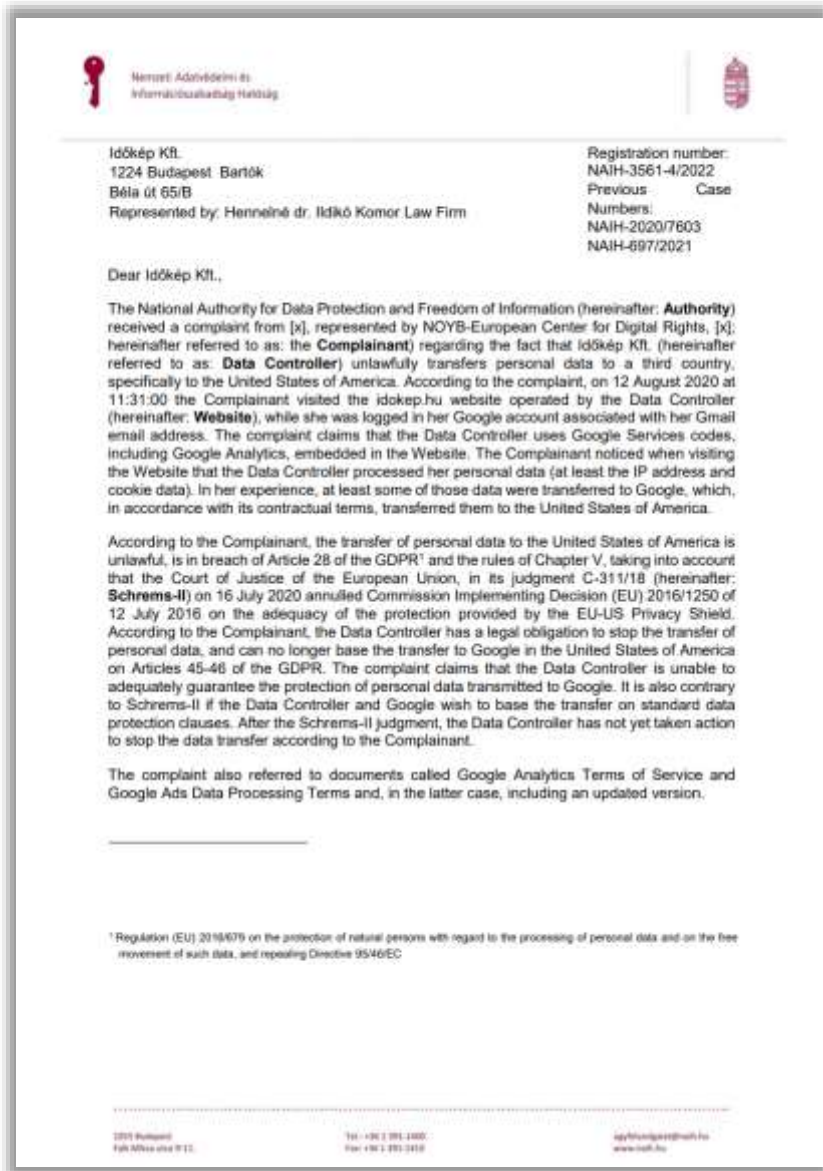


## 549 Использование сервиса Google Analytics признали незаконным в Италии

Итальянский надзорный орган в сфере защиты персональных данных, Garante per la protezione dei dati personali, 23.06.2022 признал незаконным использование компанией Caffaina Media, как владельцем веб-сайта [www.caffeinamagazine.it](http://www.caffeinamagazine.it), статистического сервиса Google Analytics трансграничной передачи персональных данных компании Google LLC, расположенной в США, при отсутствии гарантий, предусмотренных главой V GDPR. Компания была признана виновной в нарушении ст. 5(1)(a), 5(2), 13(1)(f), 24, 44 и 46 GDPR, получила административный и предписание привести обработку данных в соответствие с GDPR в течение 90 дней.

Важные аспекты решения DPA:

- Caffaina Media использовала Google Analytics в его бесплатной версии для достижения чисто статистических целей и не применила функцию "IP-анонимизации". При этом IP-адрес является персональными данными, и функция "IP-анонимизации", предлагаемая Google, является скорее методом псевдонимизации, чем анонимизации, учитывая возможности Google по обогащению персональных данных за счет дополнительной информации, которой он располагает.
- Механизмы шифрования передаваемых в США данных недостаточны для того, чтобы избежать риска доступа к данным, переданным из ЕС, государственными органами США, поскольку такие методы шифрования предусматривают, что ключ шифрования остается в руках Google, который владеет им, как импортер, в силу необходимости иметь данные в открытом виде для осуществления обработки и предоставления услуг. При этом обязательство по предоставлению доступа со стороны властей США ложится на Google не только в отношении импортированных персональных данных, но и в отношении любых криптографических ключей, необходимых для того, чтобы сделать их понятными. Таким образом, до тех пор, пока ключ шифрования остается в распоряжении импортера, принятые меры не могут считаться адекватными.
- Все итальянские владельцы веб-сайтов, как государственных, так и частных, были призваны принять во внимание незаконность передачи данных в США в результате использования Google Analytics в текущей конфигурации данного сервиса.



Noyb - Европейский центром цифровых прав, подал жалобу в венгерский орган по защите данных (Nemzeti Adatvédelmi és Információszabadság Hatóság - NAIH), утверждая, что контроллер передал персональные данные, включая IP-адрес, компании Google Ireland и, в конечном итоге, Google LLC в США посредством сервиса Google Analytics.

NAIH отметил, что согласно устоявшейся трактовке ЕС, IP-адреса являются персональными данными. NAIH также подтвердил, что, поскольку контроллер самостоятельно принимал решение о том, будет ли он использовать услуги, требующие установки cookies, статус контроллера как "контроллера данных" был правильным в соответствии со ст.4(7) GDPR.

Ст.44 GDPR требует, чтобы передача персональных данных третьей стране или международной организации для обработки могла происходить только при условии соблюдения положений главы V GDPR. Обнаружив, что контроллер по-прежнему передает персональные данные в США без оснований на одном из этих положений, DPA предписал контроллеру прекратить передачу.

## 551 Датский Datatilsynet считает использование Google Analytics незаконным



Датский орган по защите данных ("Datatilsynet") 21.09.2022 объявил, что после изучения Google Analytics, его настроек и условий, он пришел к выводу, что этот инструмент не может использоваться законно. Datatilsynet заявил, что его решение вписывается в общеевропейскую позицию надзорных органов по использованию Google Analytics. В связи с этим Datatilsynet отметил, что датские организации, использующие Google Analytics, должны оценить, соответствует ли это GDPR, и, если нет, то они должны внедрить дополнительные технические, организационные и правовые меры. В связи с этим Datatilsynet уточнил, что одной из возможных технических мер, которую могут использовать организации в качестве дополнительной меры, является псевдонимизация.

Datatilsynet отметил, что он не может исключить, что могут существовать обстоятельства или технические параметры, которые он не принял во внимание, и поэтому приглашает организации и лиц, обладающих особым пониманием соответствующего инструмента, написать в Datatilsynet здесь, если они считают, что существуют обстоятельства, которые Datatilsynet не принял во внимание. Кроме того, Datatilsynet опубликовал вопросы и ответы ("[Q&A](#)") по использованию Google Analytics и дополнительную информацию о решениях надзорных органов.

<https://www.datatilsynet.dk/english/google-analytics/use-of-google-analytics-for-web-analytics>

<https://www.datatilsynet.dk/english/google-analytics>



### Varsel om vedtak i Google Analytics-saken

Datatilsynets foreløpige konklusjon er at bruk av Google Analytics ikke er i tråd med *personvernforordningen*. Partene i sakene får mulighet til å uttale seg i saken før vi fatter et formelt vedtak.

Organisasjonen noyb har klaget inn en rekke europeiske nettsider til datatilsynsmyndighetene i EØS. Bakgrunnen er at noyb mener nettsidene overfører personopplysninger ut av EØS i strid med personvernforordningen (GDPR) ved å bruke det amerikanske analyseverktøyet Google Analytics.

Et av de innklagede nettstedene, telenor.com, er norsk og brukte tidligere Google Analytics. Datatilsynet har derfor undersøkt denne saken. Vår foreløpige konklusjon er at bruk av Google Analytics var i strid med GDPRs overføringsregler. Vi har nå sendt et forhåndsvarsel til partene i saken, slik at de får mulighet til å kommentere funnene før vi fatter et vedtak.

### Europeisk koordinering

Siden det har kommet så mange klager om bruk av Google Analytics på europeisk nivå, har Det europeiske *personvernrådet* (EDPB) opprettet en egen arbeidsgruppe for å koordinere klagesaksbehandlingen. Datatilsynsmyndighetene har nemlig plikt til å tolke GDPR likt i hele EØS.

Норвежский орган по защите данных ("Datatilsynet") 01.03.2023 опубликовал предварительное решение об использовании Google Analytics компанией Telenor ASA. Сайт норвежской компании Telenor был одним из тех сайтов, на которые была направлена жалоба НКО «None of Your Business» ("NOYB"), утверждавшей о незаконности передачи персональных данных в США через Google Analytics.

Datatilsynet пришел к предварительному выводу о том, что использование компанией Telenor системы Google Analytics было осуществлено в нарушение положений о трансграничной передаче данных в соответствии с GDPR. На момент подачи жалобы на сайте Telenor использовался Google Analytics 3, поэтому Datatilsynet уточнил, что его расследование касается исключительно этой версии Google Analytics. Однако Datatilsynet считает, что Google Analytics 4 не обязательно устраняет проблемы, присущие Google Analytics 3.





Шведский орган по защите данных (ИМУ) 03.07.2023 объявил о принятии мер против четырех компаний за незаконную передачу персональных данных в США с помощью Google Analytics после получения жалоб от НКО "Не ваше дело" (NOYB). В частности, ИМУ оштрафовал компанию Tele2 Sverige AB на €1 млн. и местного онлайн-ритейлера CDON AB - на € 25 тыс., а также вынес предписания компаниям Coop Sverige AB и Dagens Industri Aktieföring о прекращении использования Google Analytics.

Все четыре компании основывали свою передачу персональных данных в США с использованием Google Analytics на стандартных договорных положениях (SCC). Однако, ни дополнительные меры, принятые каждой компанией, ни меры, принятые Google LLC, не были достаточно эффективными, чтобы предотвратить получение спецслужбами США доступа к персональным данным. Таким образом, ИМУ признал Tele2, CDON, Coop Sverige и Dagens нарушившими ст.44 GDPR.

## 554 Использование сервиса Google Analytics признали законным (!) в Испании

15.12.2022 испанский орган за защите данных ("AEPD") опубликовал свое решение по использованию Google Analytics Испанской королевской академией ("RAE") и представил критерии, отличающиеся от критериев других более жестких европейских органов (включая французские, австрийские, датские и голландские органы по защите данных). AEPD пришел к выводу, что использование Google Analytics не связано с нарушением GDPR. Он указал, что RAE не использует эту информацию для идентификации веб-пользователей. Решение основано на следующем:

- RAE использовало бесплатную версию инструмента.
- RAE не использовало ни одну из опций предварительного информирования, доступных в Google Analytics (или Google Signals/Comparatives), которые требуют утвердительной активации. Использовались только основные функциональные возможности Google Analytics, минимизируя воздействие на конфиденциальность пользователей, так что не обрабатывалась информация, относящаяся к идентифицированным или идентифицируемым лицам, а только агрегированная информация.
- Использование Google Analytics было ограничено только и исключительно доступом к статистической и агрегированной информации, которая не позволяет идентифицировать пользователей.
- Не было получено никаких данных, которые можно было бы считать персональными данными (RAE заявляет, что не осуществляла никакой деятельности по обработке, связанной с IP-адресом), поскольку не обрабатывалась информация, которая прямо или косвенно идентифицирует или позволяет идентифицировать этих пользователей.
- Единственной информацией, которая могла бы индивидуально идентифицировать пользователей, была бы информация, связанная со случайным идентификатором, который Google присваивает своим пользователям. На основании этой информации RAE не может предпринять никаких действий для повторной идентификации пользователей.
- Правовые отношения между RAE и Google являются отношениями контроллера и обработчика данных соответственно.
- Факт того, что RAE прекратило использование инструмента после решения по делу Schrems II.

Хотя в решении отсутствует подробный анализ мер, применяемых RAE при использовании инструмента, не говоря уже об аргументации AEPD, оно устанавливает веху: простое использование инструментов американских компаний не может считаться запрещенным или осуждаться из-за того, что они предоставляются американскими организациями. Это важный прецедент, открывающий дверь для использования Google Analytics (или аналогичных инструментов) испанскими организациями.

## Датский Datatilsynet запретил муниципалитетам использование Chromebook и Google Workspace

**DATATILSYNET**

### Datatilsynet nedlægger behandlingsforbud i Chromebook-sag

Dato: 14-07-2022  
Nyhed

I en sag om brug af Chromebooks i Helsingør Kommune udtaler Datatilsynet alvorlig kritik og nedlægger forbud mod overførsel til tredjelande og mod brugen af Google Workspace.



Datatilsynet har gennem længere tid haft fokus på brugen af Chromebooks og Google Workspace (tidligere G Suite for Education) i kommunerne. Brugen er udbredt på landsplan, men konkret har Datatilsynet haft en vespærende sag i Helsingør Kommune.

Således traf Datatilsynet en afgørelse i september 2021, hvor Helsingør Kommune bl.a. fik et påbud om at foretage en risikovurdering af kommunens behandlinger af personoplysninger i folkeskolen ved brug af Chromebooks og Workspace. Datatilsynet har nu på baggrund af den dokumentation og vurdering af risikoen for de registrerede, som Helsingør Kommune har udført, konstateret, at behandlingen ikke lever op til kravene i GDPR på flere punkter.

В сентябре 2021 года датский орган по защите данных (Datatilsynet) приказал муниципалитету Хельсингёра провести оценку риска обработки персональных данных (DPIA) в начальной школе с использованием Chromebook и Workspace.

По результатам проведенного DPIA Datatilsynet установил, что указанная обработка данных не соответствует требованиям GDPR по нескольким пунктам, в т.ч. касаясь трансграничной передачи персональных данных в США.

Муниципалитет Хельсингёра получил предписание до 03.08.2022:

- прекратить использование Chromebook и Workspace;
- потребовать у Google уничтожить ранее полученные персональные данные;
- обратиться к родителям учеников начальной школы с просьбой удалить персональные данные из используемых ими Chromebook и Workspace.

Datatilsynet дополнительно обратил внимание, что:

- неисполнение предписания грозит виновным лицам лишением свободы до 6 месяцев;
- ожидает от других муниципалитетов Дании, использующих Chromebook и Workspace, следование предписанию.

18.08.2022 Datatilsynet опубликовал решение, в котором признал муниципалитет Хельсингёра нарушившим ст.35(1), 35(7), 36(1) GDPR после рассмотрения пояснений, которые муниципалитет направил в Datatilsynet 01.08.2022.


Datatilsynet оставил в силе свой запрет от 14.07.2022 на использование муниципалитетом Google Workspace. Запрет действует до тех пор, пока муниципалитет не приведет свою деятельность по обработке данных в соответствие с GDPR и не проведет DPIA в соответствии со ст.35 и 36 GDPR.

<https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag>

[https://edpb.europa.eu/news/national-news/2022/danish-dpa-imposes-ban-use-google-workspace-elsinore-municipality\\_en](https://edpb.europa.eu/news/national-news/2022/danish-dpa-imposes-ban-use-google-workspace-elsinore-municipality_en)

<https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/aug/ny-afgoerelse-datatilsynet-fastholder-forbud-i-chromebook-sag>

## Ограничение использования Chrome OS и браузера Chrome в учреждениях образования в Нидерландах



Ministerie van Onderwijs, Cultuur en Wetenschap

**TER ONDERTEKENING**  
Aan: MPVO

**nota**

Naar aanleiding van gesprek met MPVO op 22/06/2022 over de Kamerbrief over digitale weerbaarheid

**Aanleiding**

U ontvangt deze nota naar aanleiding van ons gesprek op 22 juni 2022 over de Kamerbrief over digitale weerbaarheid waarin u heeft verzocht om scherper inzicht te bieden in de effectiviteit van onze aanpak/Plan Veilig Digitaal Onderwijs, de rol van OCW, het normerend karakter en wat dit vraagt in wet- en regelgeving, de verdeling van taken en verantwoordelijkheden van alle partijen, het tijdpad (fasering en mijlpalen), de kwaliteitscontrole, monitoring en evaluatie. Ter informatie sturen wij u als bijlagen de verkenning naar het normenkader voor het funderend onderwijs van Berenschot en het normenkader voor het hoger onderwijs en in het middelbaarberoepsonderwijs waarop we ons in het po en vo baseren.

**Kernpunten**

We hebben de kamerbrief aangescherpt langs de door u benoemde volgende uitgangspunten:

- **Integrale aanpak:** met de totale aanpak borgen we een veilig digitaal funderend onderwijs. De uitvoering vindt gefaseerd plaats.
- **Meer centrale regie:** scholen kunnen het niet alleen en daarom gaan we risicogericht helpen.
- **Normstelling:** scholen moeten weten waar ze minimaal aan moeten voldoen, hoe ze daaraan kunnen voldoen, en hoe ze worden gecontroleerd en waar nodig met welke sancties. Dit gaan we communiceren (bewustwording). Daarnaast voeren we een nulmeting uit (waarmee we zicht hebben op de zwakke plekken in de sector en waar scholen nu staan qua cyberdreigingsbeeld), monitoren en benchmarken we periodiek, stellen we het normenkader bij waar nodig op basis van het dreigingsbeeld, en zien we erop toe dat scholen eraan voldoen en grijpen waar nodig in.
- **Helpen:** we gaan scholen ondersteunen met raad en daad en beschermen waar ze risico's over het hoofd zien
- **Publieke voorzieningen:** de overheid regelt centrale voorzieningen waar keten/coördinatieproblemen optreden en schaalvoordelen evident te behalen zijn.
- **Fasering:** we starten nu met communicatie, normstelling, en hulp bij incidenten. Tegelijkertijd bereiden we de volgende stappen voor die de basisinfrastructuur betreffen (ICTU onderzoek, beleidsadvies ict-)

Pagina 1 van 4

**Primaire Onderwijs**

**Van** [Redacted]

**Datum** 27 juni 2022

**Referentie**

**Bijlagen**  
Kamerbrief digitale weerbaarheid onderwijs en onderzoek (school)  
Kamerbrief digitale weerbaarheid onderwijs en onderzoek (back channel)  
Normenkader HO  
Verkenning Berenschot normenkader TRF PO

Министерство образования Нидерландов ввело ограничение на использование Chrome OS и браузера Chrome до августа 2023 года. Чиновники обеспокоены приватностью данных студентов и не до конца понимают, как компания использует персональные данные.

Образовательные учреждения и школы, которые всё равно хотят продолжать использовать сервисы Google, должны будут выполнить рекомендации SURF. В частности, отключить такие службы, как автоматический перевод веб-сайтов и проверка орфографии, которые могут привести к утечке пользовательских данных. Кроме того, географическое расположение для хранения данных Google Cloud должно быть установлено на Европу, а пользователям нельзя изменять настройку. Наконец, персонализация рекламы должна быть отключена, встраивание YouTube должно использоваться в «режиме повышенной конфиденциальности», а поисковая система Google должна быть полностью исключена.

### Germany Forces a Microsoft 365 Ban Due to Privacy Concerns

By Vuk Mijovic / September 23, 2022



Germany has proclaimed a partial Microsoft 365 ban in 2018 and has been holding it since.  
Source: Maheshkumar Painam via Unsplash.com

The central German state of Hesse's local Data Protection Authority (DPA) has banned the use of Microsoft 365 in its schools, citing concerns over privacy violations. According to the authority, the program's settings gather data from within the users' programs. This clearly violates the EU's General Data Protection Regulation (GDPR) policies.

The Microsoft 365 debate has been a longstanding one in Germany. In 2018, several state courts, including the federal German court, found that Microsoft violated local laws connected to the GDPR. From there, the Microsoft 365 ban spread to France. The ban has mostly affected educational institutions and companies that work with these programs.

Управление по защите данных (DPA) немецкой земли Гессен запретило использование Microsoft 365 в местных школах, ссылаясь на опасения по поводу нарушения прав субъектов путем сбора их пользовательских данных, что противоречит требованиям GDPR. Запрет был введен после того, как Microsoft прекратила действие специального соглашения для немецких пользователей. Согласно этому соглашению, Microsoft разрешала локальное хранение пользовательских данных в Германии. Это гарантировало, что данные пользователей не покинут пределы страны.

После прекращения действия этих договоренностей и законодательных изменений в США перед Microsoft 365 в ЕС теперь стоят три основные проблемы:

- ✳️ **Власти ЕС требуют хранения в ЕС данных несовершеннолетних пользователей.**

- ✳️ **Согласно принятому в США CLOUD Act, американские спецслужбы могут получить доступ к пользовательским данным, хранящимся на серверах американских компаний, даже к данным неграждан США.**

- ✳️ **Microsoft не гарантирует защиту данных несовершеннолетних пользователей, в т.ч. возможность отключить сбор их данных.**

Решение для компаний, работающих внутри Европы, заключается в приобретении локальных лицензий и отказа от облачной версии ПО.

## Немецкий DSK: использование Microsoft 365 (включая Office 365) по-прежнему не соответствует GDPR



Любой, кто использует Microsoft 365 (включая Office 365) в Германии, нарушает европейское законодательство GDPR - по крайней мере, в том, что касается стандартной конфигурации, указанной Microsoft. Несмотря на последующие усовершенствования, Microsoft пока не удалось обеспечить соответствие Microsoft 365 требованиям GDPR. К такому выводу пришли участники конференции (Datenschutzkonferenz, DSK) независимых органов по защите данных федерального правительства и правительств земель Германии.

Так, продукты, содержащиеся в Microsoft 365, не могут использоваться в школах, учебных заведениях и компаниях таким образом, чтобы это соответствовало требованиям защиты данных и, следовательно, закону.

Центральным и повторяющимся вопросом в серии обсуждений был вопрос о том, в каких случаях Microsoft действует как процессор, а в каких - как контроллер. Это не удалось окончательно прояснить. Контроллеры должны быть в состоянии постоянно выполнять свои обязательства по отчетности в соответствии со ст.5(2) GDPR. При этом Microsoft не полностью раскрывает, какие операции по обработке данных имеют место.

## Q&A от CNIL по использованию систем интернет-статистики в контексте решения CJEU 'Schrems II' (1/2)

Французская национальная комиссия по информатике и свободам (CNIL) 07.06.2022 опубликовала Q&A в отношении использования Google Analytics, а также руководство по правомерному использованию других систем анализа поведения посетителей интернет-ресурсов в контексте решения CJEU 'Schrems II'.

### Неэффективные практики

✳ Попытка сконфигурировать настройки Google Analytics таким образом, чтобы пользовательские данные не передавались из ЕС в США или чтобы в США передавались только анонимные данные.

✳ Шифрование является достаточной защитой только в той мере, в какой экспортер данных имеет исключительный контроль над ним, в то же время Google сам шифрует собираемые Google Analytics пользовательские данные и может получить к ним доступ или предоставить его по запросу спецслужб США.

может являться использование прокси-сервера для передачи данных в системы аналитики вне ЕС/ЕЭЗ при условии, что такой сервер должен соответствовать следующим условиям:

отсутствие передачи IP-адреса на серверы вне ЕС/ЕЭЗ;

подмена идентификатора пользователя прокси-сервером, алгоритм которого должен обеспечивать достаточный уровень коллизии (т.е. достаточно низкую вероятность того, что два разных идентификатора дадут одинаковый результат после хэширования) и включать компонент, изменяющийся во времени (добавление значения к хэшированным данным, которое изменяется со временем, так что результат хэширования не будет всегда одинаков для одного и того же идентификатора);

удаление внешней по отношению к интернет-ресурсу информации о ссылающемся на него сайте;

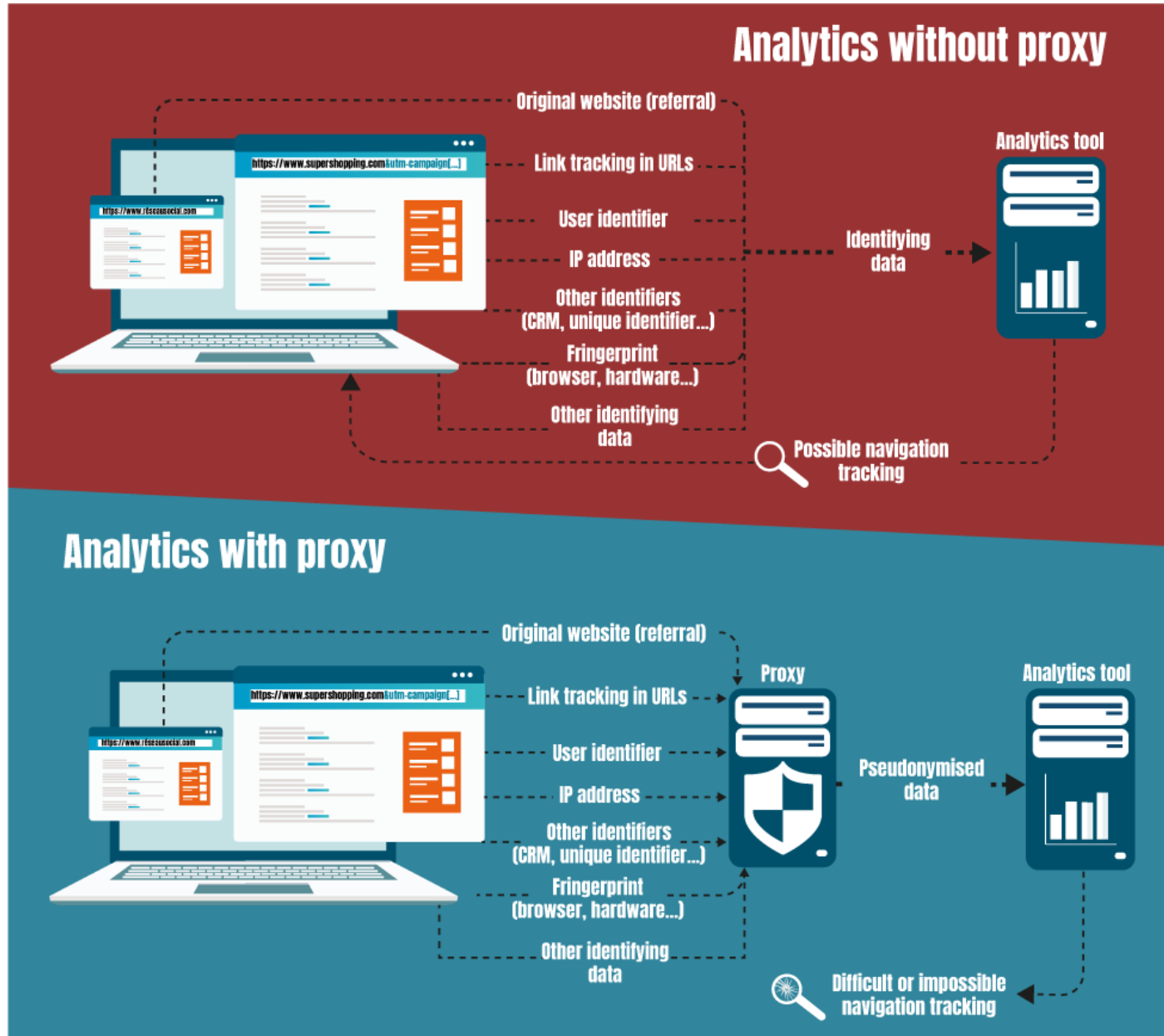
удаление любого параметра, содержащегося в собранных URL-адресах (например, UTM и параметры URL-адресов, обеспечивающие внутреннюю маршрутизацию интернет-ресурса);

переработка сведений, могущих быть использованными в создании цифрового отпечатка (например, «пользовательские агенты» - user agents), для удаления самых редких конфигураций, которые могут привести к реидентификации пользователя;

отсутствие какого-либо набора межсайтовых идентификаторов (CRM ID, уникальный ID);

удаление любых других данных, которые могут привести к реидентификации пользователя.

✳ **Хостинг прокси-сервера должен гарантировать отсутствие передачи входящих «сырых» данных за пределы ЕС (до момента их обработки – как указано выше) – см. следующий слайд.**





## 561 Разъяснения датского Datatilsynet о концепции «экспортеров данных»



Датский орган по защите данных ("Datatilsynet") опубликовал 08.06.2022 разъяснения о концепции "экспортеров данных", которые адресованы контроллерам, использующим европейских процессоров, но при этом один или несколько их субпроцессоров находятся за пределами ЕС/ЕЭЗ, а также процессорам в ЕС/ЕЭЗ, которые предоставляют услуги, используя субпроцессоров за пределами ЕС/ЕЭЗ. В отношении передачи данных ст.44 GDPR налагает обязательство как на контролеров, так и на процессоров, где обе стороны обязаны обеспечить эффективное основание для передачи данных.

Возникает много вопросов, когда европейский контроллер использует одного или нескольких процессоров в пределах ЕС/ЕЭЗ, а один или несколько его субпроцессоров находятся за пределами ЕС/ЕЭЗ. Благодаря новым SCC, процессор может заключить договор напрямую с любым субпроцессором в третьих странах, чтобы обеспечить необходимое основание для передачи в соответствии со ст.46(2)(c) GDPR. В таких случаях именно обработчик называется "экспортером данных" и непосредственно связан положениями стандартного договора и его содержанием.

Кроме того, на практике за контроллером остается обязанность обеспечить и быть в состоянии продемонстрировать органу власти, что процессор установил необходимую основу для передачи и что эта основа для передачи является эффективной в свете всех обстоятельств передачи, включая реализацию дополнительных защитных мер.

## Разъяснения немецкой DSK о доступе государственных органов третьих стран к персональным данным в ЕС/ЕЭЗ

Немецкая конференция по защите данных ("DSK") 31.01.2023 утвердила разъяснения об оценке защиты данных при доступе государственных органов третьих стран к персональным данным. DSK оценила возможности доступа государственных органов третьих стран к персональным данным, обрабатываемым компанией, расположенной в ЕС/ЕЭЗ, в соответствии со ст.28 GDPR. Одного лишь риска того, что государственные органы третьей страны или материнская компания компании из ЕС/ЕЭЗ в третьей стране могут дать ей указание передать персональные данные в третью страну, недостаточно, чтобы считать, что передача данных в третью страну по смыслу ст.44 GDPR имела место.

DSK указала, что такой риск может привести к сомнению в надежности процессора в соответствии со ст.28(1) GDPR, если процессор или контроллер не приняли технические или организационные меры, которые обеспечивают достаточные гарантии того, что процессор будет соблюдать свои обязательства, особенно в отношении воздержания от обработки вопреки инструкциям контроллера, особенно на основании обязательств законодательства третьей страны.

В той степени, в которой существует риск того, что практика или норма, которая может требовать незаконной обработки в соответствии с законодательством ЕС, также применима к дочерней компании ЕЭЗ компании третьей страны, такая обработка дочерней компанией в качестве процессора сама по себе не является достаточной для достижения надежности в соответствии со ст.28(1) GDPR. В этом контексте ДСК выразил мнение, что к тщательности проверки надежности в соответствии со ст.28(1) GDPR должны предъявляться особенно высокие требования. В случае, если процессор не в состоянии предоставить достаточные гарантии после выявления вышеупомянутых рисков, контроллеры могут обратиться к Рекомендациям 01/2020 Европейского совета по защите данных ("EDPB") за помощью в отношении технических и организационных мер, которые могут быть предприняты для устранения выявленных недостатков.

<https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html>

[https://www.datenschutzkonferenz-online.de/media/dskb/20230206\\_DSK\\_Beschluss\\_Extraterritoriale\\_Zugriffe.pdf](https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf)

## **В Норвегии больницы не несут ответственности за медицинские данные после их разглашения иностранным лабораториям**

Норвежский совет по конфиденциальности («Personvernemnda») опубликовал 03.05.2022 года свое решение по делу № PVN-2021-21, в котором он постановил, что Oslo universitetssykehus HF («Университетская больница Осло») не несет ответственности за данные о состоянии здоровья пациентов после того, как они были медицинскому персоналу в иностранных лабораториях.

Дело касается жалобы Университетской больницы Осло на решение норвежского органа по защите данных ("Datatilsynet") от 26.04.2021, в котором Datatilsynet предписал больнице урегулировать раскрытие ею медицинской информации иностранным лабораториям в отдельных соглашениях об обработке данных (DPA) в соответствии со ст.28 GDPR или в соглашениях о совместном контроле (JCA) в соответствии со ст.26 GDPR. Основной спорный момент заключается в том, остается ли больница контролером данных, предоставляемых иностранным лабораториям

Personvernemnda постановил, что правила, применяемые к обмену медицинской информацией с иностранными лабораториями на территории ЕС или ЕЭЗ, будут такими же, как и при отправке норвежским врачом медицинской информации в норвежские лаборатории, или при обмене данными между больницами в Норвегии, или при передаче данных зарубежным провайдерам медицинских услуг. Правила сотрудничества с медицинскими партнерами за рубежом, включая иностранные лаборатории, не могут быть более строгими, чем национальные правила, которые применяются к таким партнерам в соответствии со ст.1(3) GDPR.

Personvernemnda заключил, что доступ контролера, а во многих случаях и обязанность раскрывать медицинскую информацию медицинскому персоналу в иностранных лабораториях, исчерпывающе регулируется законодательством о здравоохранении, и что не может быть выдвинуто дополнительное требование о заключении соглашения в соответствии со ст. 26 и 28 GDPR.

Предписание Datatilsynet в адрес Университетской больницы Осло о заключении DPA или JCA было отменено.

## Facebook Meta может получить предписание ирландской DPC временно приостановить передачу данных в США

### THE IRISH TIMES

#### Facebook's Meta facing order from Irish regulator to suspend data transfers to US

Wide-ranging privacy case has already led to threats from social media giant

© Tue, Feb 22, 2022, 05:38



Facebook owner Meta has already threatened to pull its websites from Europe. Photograph: Chris Delmas/AFP via Getty Images

Facebook owner Meta is facing an imminent order from Ireland's data regulator to suspend data transfers to the United States, in a far-reaching privacy case that has already led to threats from the social media giant to pull its websites from Europe.

Data protection commissioner Helen Dixon sought the suspension in a draft ruling against Meta on Monday, starting the clock on a high-stakes legal process in which the final decision will be subject to the approval of her European counterparts.

Ирландская Комиссия по защите данных в феврале 2022г. ознакомила Facebook с проектом предписания о временном приостановлении трансграничной передачи данных европейских пользователей в США – до момента завершения панъевропейского расследования в отношении Facebook. В соцсети подтвердили факт получения документа.

## Отказ суда признать использование Amazon Web Services как несовместимое с решением по делу «Schrems II»

12.03.2021 Государственный совет (Conseil d'Etat) - высший административный суд Франции - постановил, что персональные данные на платформе, используемой для бронирования вакцинации от COVID-19, управляемой Doctolib и размещенной на Amazon Web Services, в достаточной степени защищены согласно требованиям GDPR и контрактным оговоркам, согласно которым были введены достаточные юридические и технические меры защиты данных в случае получения запроса о доступе от властей США. Таким образом, был отклонен иск профессиональных ассоциаций и союзов медицинских работников о запрете на использование американского сервиса AWS, что создавало угрозу противоправного доступа к данным граждан ЕС в соответствии с решением Суда Европейского Союза «Schrems II».

Суд отметил, что для целей размещения своих данных Doctolib использует услуги люксембургской компании AWS Sarl, данные размещаются в ЦОДах, расположенных во Франции и Германии, а договор, заключенный между Doctolib и AWS Sarl, не предусматривает передачи данных в США. Однако, поскольку в соответствии с законодательством США, AWS Sarl это дочерняя компания Amazon, суд счел, что AWS Sarl в Люксембурге может быть обязано исполнять запросам на доступ к данным со стороны властей США в рамках программ мониторинга США на основании статьи 702 Закона США об иностранных государствах, Закона о разведывательном надзоре или Постановления 12333.

В то же время суд установил, что предложенный AWS Sarl в адрес Doctolib уровень защиты данных был достаточным из-за множества действующих гарантий, которые были указаны контракте на оказание услуг:

**Правовые гарантии** – контракт предусматривает особую процедуру в случае получения AWS Sarl запроса на доступ к данным от иностранного органа государственной власти; в частности, AWS Sarl гарантирует, что он будет оспаривать любой поступивший от иностранных государственных органов запрос на доступ к данным.

**Технические меры безопасности** – технически данные, размещенные на AWS Sarl, зашифрованы, а ключ хранится у доверенной третьей стороны во Франции, а не у AWS, что предотвращает возможность несанкционированного доступа к данным со стороны третьих лиц.

### Прочие гарантии:

- **Отсутствие данных о состоянии здоровья** – данные, получаемые Doctolib в рамках кампании вакцинации, не касаются информации о причине, по которой данное лицо имеет право на вакцинацию в приоритетном порядке из-за специфических патологий. Размещенные в AWS данные необходимы только для идентификации людей с целью их записи на прием.
- **Данные удаляются через три месяца** – данные автоматически удаляются не позднее, чем через три месяца с даты осуществления записи на вакцинацию, и субъектам также предоставляется возможность удалить свои данные раньше этого срока посредством сайта в Интернете.

## Суд Висбадена наложил временный судебный запрет на использование сервиса управления файлами cookie

01.12.2021 Административный суд Висбадена вынес первое в своем роде решение (временный судебный запрет), постановившее, что компании не могут использовать поставщика сервиса по управлению файлами cookie на веб-сайте, который использует размещенную в США службу сбора пользовательских данных, независимо от того, действительно ли сами пользовательские данные покидают пределы ЕС.

Рейнско-Майнский университет прикладных наук (RMU) интегрировал на своем веб-сайте сервис управления файлами cookie «Cookiebot» датской компании Cybot. Cookiebot отображает баннер, который позволяет пользователю установить свои предпочтения в отношении файлов cookie. Когда пользователь делает это, Cookiebot собирает, среди прочего, IP-адрес пользователя, URL-адрес, определяемый предпочтениями пользователя (например, веб-сайт RMU), и уникальный случайный «пользовательский ключ», назначенный пользователю. Ключ пользователя и настройки хранятся локально, поэтому сайт RMU продолжает учитывать пользовательские настройки. Cookiebot также хранит все вышеперечисленные данные в собственной базе данных. Согласно Cookiebot, это делается для того, чтобы — в соответствии с требованиями GDPR — у компании были наглядные доказательства согласия пользователей на хранение файлов cookie.

Предполагаемая проблема заключалась в том, что Cookiebot использовал американскую сеть доставки контента (Akamai Technologies) для сбора этих данных. Важно отметить, что суд Висбадена, похоже, согласился с тем, что Akamai могла хранить данные Cookiebot на серверах в ЕС, а не в США, что предполагает соглашение Cookiebot с немецким филиалом Akamai. Но суд, в т.ч. с учетом пояснений Комиссии по защите данных земли Гессен, постановил, что это не имеет значения. Он постановил, что простое использование американского провайдера для сбора данных об IP-адресах и ключах пользователей является незаконной «передачей», поскольку:

- Согласно практике Суда Европейского Союза, IP-адреса являются персональными данными (суд также посчитал персональными данными «пользовательский ключ» Cookiebot).
- В соответствии с законодательством США (Clarifying Lawful Overseas Use of Data Act — CLOUD Act) поставщик облачных услуг в США может быть обязан предоставить все данные, находящиеся в его владении, на хранении или под контролем, правоохранительным органам США, независимо от того, хранятся ли данные в США или за их пределами.

<https://rewis.io/urteile/urteil/2tj-01-12-2021-6-l-73821wi/>

<https://iapp.org/news/a/new-eu-data-blockage-as-german-court-would-ban-many-cookie-management-providers/>

## Тюрингский TLfDI обратил внимание риски, связанные с использованием Google Fonts



### Pressemitteilung

#### Schriftarten sind nicht so banal, wie viele denken: Google Fonts löst Abmahnwelle aus

Erfurt, 18. August 2022: Aus aktuellem Anlass möchte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse über Folgendes informieren:

**Drohende Abmahnwelle?** Laut Medienquellen soll es aktuell zu einer Abmahnwelle gegen tausende von Websites-Betreibern kommen. Grund ist die dynamische Einbettung von Google Fonts auf deren Website, ohne vorab die Einwilligung der Besucher der Website einzuholen. Auch beim TLfDI gehen regelmäßig Beschwerden dieses Inhalts gegen Seitenbetreiber ein. Bei einer dynamischen Einbindung werden die Schriftarten von Servern des US-Konzerns in den Browser des Besuchers geladen und dabei personenbezogene Daten, wie z. B. die IP-Adresse der Benutzer, in die USA übermittelt. Dies verstößt laut dem Urteil des Landgerichtes München v. 20. Januar 2022, Az. 3 O 17493/20, gegen das allgemeine Persönlichkeitsrecht und die Datenschutz-Grundverordnung. Details finden sich in den Urteilsgründen, abrufbar unter:

<https://www.gesetze-bayem.de/Content/Document/Y-300-Z-BECKRS-B-2022-N-612?hl=true>

**Worum geht es genau bei Google Fonts?** Google Fonts sind kostenlose Schriftarten des US-Konzerns Google, welche zur freien Verfügung stehen. Dabei ist es nicht jedem Website-Betreiber bekannt, dass Google Fonts auch durch eingebettete Google-Dienste (z. B. Google Maps, reCAPTCHA) automatisch mitgeladen werden.

Der Europäische Gerichtshof entschied bereits in seinem Urteil vom 16. Juli 2020 (C-311/18 „Schrems II“), dass das US-Recht derzeit den Schutz personenbezogener Daten von Bürgern aus der EU nicht angemessen gewährleistet und erklärte den sog. „Privacy Shield“ für ungültig. Demnach gelten die USA im datenschutzrechtlichen Sinne als

Postanschrift: Postfach 900455 99117 Erfurt	Dienstgebäude: Häßlerstraße 8 99096 Erfurt	Telefon: 0361 57-31 12900 E-Mail: <a href="mailto:postfach@datenschutz.thueringen.de">postfach@datenschutz.thueringen.de</a> Internet: <a href="http://www.tlfdi.de">www.tlfdi.de</a>
--	---	---

Umsatzsteuer-Identifikationsnummer: DE338711747

\*Die genannte E-Mail-Adresse dient nur für den Empfang einfacher Mitteilungen ohne Signatur/ Verschlüsselung und für mit PGP verschlüsselte Mitteilungen.

Тюрингский орган по защите данных ("TLfDI") 18.08.2022 года выпустил пресс-релиз, касающийся использования операторами веб-сайтов шрифтов Google - это бесплатные шрифты, предлагаемые Google, и что в случае динамической интеграции шрифты загружаются в браузер посетителя сайта, а персональные данные, такие как IP-адрес пользователя, передаются в США.

TLfDI регулярно получает жалобы на операторов веб-сайтов, касающиеся динамического внедрения шрифтов Google на их сайт без получения предварительного согласия посетителей сайта.

В связи с этим TLfDI рекомендовал операторам сайтов проверить, используют ли они Google Fonts и, если да, то как эта услуга интегрирована в сайт, посоветовав тем операторам сайтов, которые используют динамические Google Fonts, сохранять их локально, прежде чем интегрировать их в свои сайты.

### Hinweise des HBDI zu "Google Fonts"-Abmahnungen



Angesichts der aktuell stark zunehmenden Beratungsanfragen zu Abmahnungen aufgrund des Einsatzes von Google Fonts gibt der HBDI folgende Hinweise:

Viele Websitebetreiber erhalten derzeit Forderungsschreiben, in denen unter anderem Schadensersatz wegen der Online-Einbindung der Schriftarten von Google (Google Fonts) gefordert wird. Dies wird regelmäßig mit einem Urteil des Landgerichts München begründet, durch das der Betreiber einer Website unter anderem zu Schadensersatz in Höhe von 100 Euro wegen des Einsatzes von Google Fonts verurteilt wurde (LG München I, Endurteil v. 20.01.2022 – 3 O 17493/20).

Der HBDI weist darauf hin, dass im Rahmen seiner Zuständigkeit eine Beratung zu zivilrechtlichen Streitigkeiten nicht erfolgen kann und darf. Websitebetreiber, die sich gegen die erhobenen Forderungen zur Wehr setzen möchten, sollten zur Abstimmung der weiteren individuellen Vorgehensweise eine Rechtsberatung z. B. durch eine Rechtsanwaltskanzlei in Anspruch nehmen.

Гессенский орган по защите данных ("HBDI") выпустил 01.11.2022 заявление, содержащее информацию об использовании шрифтов Google. В частности, HBDI указал, что если шрифты Google интегрированы в интернет, браузер пользователя загружает эти шрифты при посещении веб-сайта и для этого обращается к серверам Google. В результате, пояснили в HBDI, личные данные пользователя передаются в Google. Кроме того, HBDI заявила, что такая обработка данных требует законного основания в соответствии со ст.6(1) GDPR, также подчеркнув, что если персональные данные передаются в третью страну, например, в США, то должны быть соблюдены требования, применимые к передаче в третьи страны, включая требования, установленные Судом Европейского союза ("СJEU") в деле Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) ("Дело Schrems II").

Таким образом, HBDI пришел к выводу, что любой, кто хочет использовать шрифты Google, должен убедиться, что все эти требования соблюдены, и рекомендовал сохранять шрифты локально на веб-сервере. Наконец, HBDI отметил, что подобные выводы применимы и к другим поставщикам шрифтов.



## Нижнесаксонский LfD Niedersachsen информирует о способе законно использовать Google Fonts



Орган по защите данных Нижней Саксонии ("LfD Niedersachsen") 24.11.2022 выпустило пресс-релиз, посвященный волне предупреждений и исков против использования Google Fonts владельцами веб-сайтов, которые были вызваны решением регионального суда Мюнхена от 20.01.2022 (LG Munich I - 3 O 17493/20). В частности, LfD Niedersachsen заявил, что согласно этому решению суд присудил истцу 100 евро в качестве компенсации за использование Google Fonts в нарушение защиты данных в рамках гражданского судопроизводства. Google Inc. предлагает шрифты для оформления веб-сайтов через Google Fonts, сервис, используемый на многих веб-сайтах, где существует два различных способа технической интеграции сервиса.

Google Fonts может быть интегрирован либо онлайн, при этом шрифты загружаются с серверов Google при посещении сайта, а личные данные пользователя сайта автоматически передаются в Google в США, либо шрифты, используемые на сайте, могут быть загружены и сохранены локально на собственном сервере пользователя сайта, что является вариантом, соответствующим нормам защиты данных и рекомендованным LfD Niedersachsen.

LfD Niedersachsen подчеркнула, что при изучении веб-сайтов регулярно обнаруживаются нарушения законодательства, в частности, в отношении интеграции сторонних сервисов, отметив, что предупреждающих писем/претензий можно благополучно избежать только в том случае, если при разработке веб-сайтов соблюдаются законодательные требования TTDSG и GDPR.

## Австрийский DSB признал компанию Google нарушившей GDPR за непрозрачность обработки данных с помощью Google Fonts

Австрийский орган по защите данных (DSB) 19.10.2023 вынес решение, в котором признал компанию Google LLC нарушившей GDPR в отношении сервиса Google Fonts.

DSB получил жалобы и запросы в связи с интеграцией Google Fonts на сайт компаний и обработкой персональных данных с помощью Google Fonts. В результате проведенного расследования DSB установил, что данные передаются на серверы Google LLC или Google Ireland Limited только в случае (повторной) загрузки шрифтов Google Fonts через сервер Google, но не в случае локальной интеграции шрифтов на сервер. В случае, когда шрифты Google не интегрируются локально, DSB, помимо прочего, разъяснил, что:

- информационное обязательство в соответствии со статьями 12(1) и 13 GDPR выполнено не полностью, поскольку IP-адреса могут, в зависимости от конкретного случая, считаться персональными данными;
- данные не во всех случаях передаются на серверы Google LLC в США, а зависят от географического положения пользователя или сервера его интернет-провайдера, и в случае возникновения спорных ситуаций поток данных должен проверяться в каждом конкретном случае;
- в результате интеграции Google Fonts на сайт Google LLC или Google Ireland Limited получает как минимум IP-адрес, HTTP-заголовок, включая "referrer" (информацию о сайте, через который пользователь перешел на текущий сайт), и "user agent" интернет-браузера;
- IP-адреса и HTTP-заголовки, включающие "referrer" и "user agent" интернет-браузера, обрабатываются отдельно;
- IP-адреса обрабатываются с целью обнаружения, предотвращения и борьбы с атаками, и в той мере, в какой IP-адреса квалифицируются как персональные данные, их обработка для указанных целей может быть обусловлена законными интересами в соответствии со статьей 6(1)(f) GDPR;
- IP-адреса, включая "referrer" и "user agent" интернет-браузера, не обрабатываются в рекламных целях.

## Земельный суд Мюнхена счёл использование Google Fonts связанным с трансграничной передачей данных

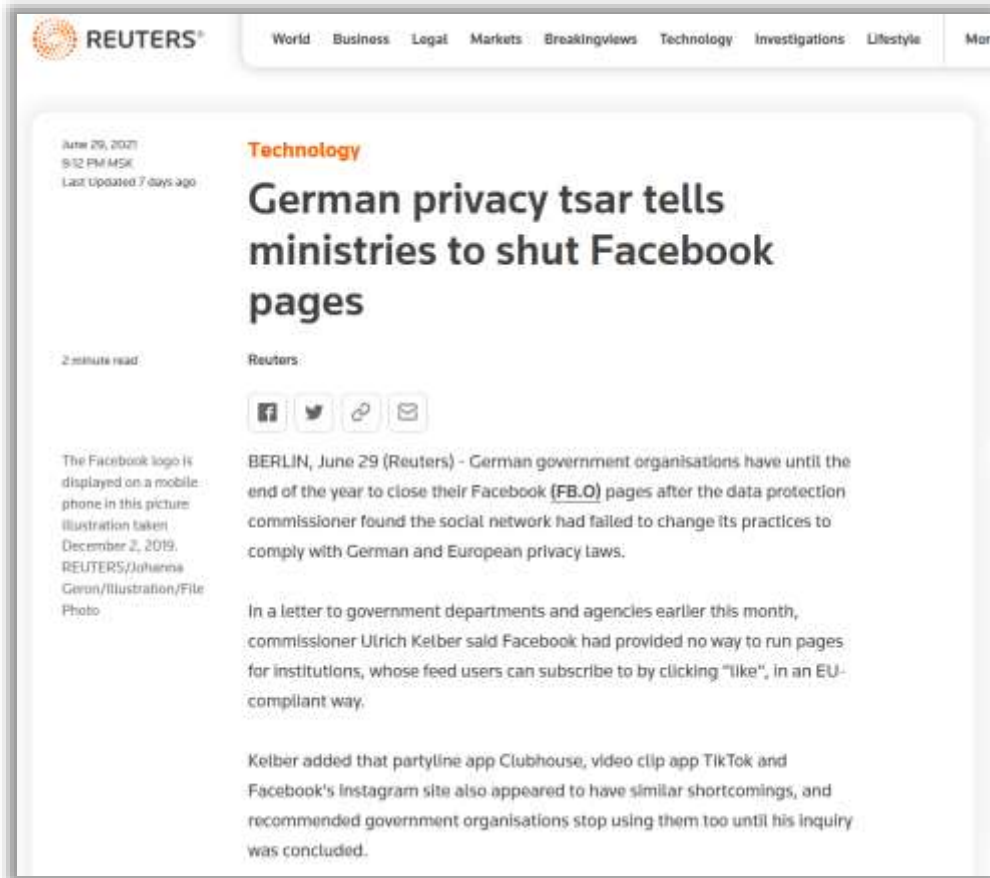
Земельный суд города Мюнхена (Германия) в своём решении от 20.01.2022г. пришел к выводу неприменимости законного интереса (legitimate interest) в качестве правового основания обработки персональных данных при использовании шрифтов Google на сайте. В перспективе это ставит под вопрос законность использования иностранных CDN (Content Delivery Network) на территории ЕС. Некоторые выводы судебного решения:

- Владельцу сайта было приказано выплатить субъекту данных небольшую компенсацию в размере €100 согласно ст.82 GDPR и предоставить субъекту данных ответ на его запрос в соответствии со ст.15 GDPR. В случае повторного нарушения сайту грозит штраф до €250,000 евро.
- Встраивание в сайт шрифтов Google Fonts означает передачу динамического IP-адреса пользователя сайта в Google.
- Динамический IP-адрес — это персональные данные. Суд опирается на доводы из судебного решения по делу *Брейера*, согласно которым существуют разумные средства для идентификации субъекта данных с помощью третьих лиц, а именно компетентного органа и интернет-провайдера.
- Надлежащих правовых оснований (например, согласие пользователя сайта) для такой передачи данных не было выявлено. Также владелец сайта не может опираться на свой законный интерес согласно ст.6(1)(f) GDPR, поскольку Google Fonts также может использоваться ответчиком без установления соединения с серверами Google при загрузке страницы.
- При расчете размера компенсации субъекту данных суд учел, что это было регулярное, а не разовое раскрытие данных. Персональные данные передавались на серверы Google в США, т.е. не имели надлежащего уровня защиты.

<https://rewis.io/urteile/urteil/lhm-20-01-2022-3-o-1749320/>

[https://www.reddit.com/r/gdpr/comments/sg8sll/no legitimate interest for using google fonts on/](https://www.reddit.com/r/gdpr/comments/sg8sll/no_legitimate_interest_for_using_google_fonts_on/)

## Правительственные организации Германии закрывают свои страницы в Facebook



Правительственные организации Германии должны до конца 2021 года закрыть свои страницы в Facebook после того, как Федеральный комиссар Германии по защите данных и свободы информации Ульрих Кельбер (BfDI) обнаружил, что социальная сеть не смогла изменить свою практику трансграничной передачи данных европейских пользователей в США в соответствии с немецкими и европейскими законами о защите персональных данных.

## Отчет IAF об осуществлении компаниями ЕС трансграничного экспорта HR-данных с учетом Schrems II и рекомендаций EDPB



Фонд информационной подотчетности (Information Accountability Foundation) опубликовал отчёт «Addressing Human Resources Data Flows in Light of European Data Protection Board Recommendations», в котором был описан актуальный опыт европейских компаний по учету последствий решения Суда Европейского Союза «Schrems II» при трансграничной передаче кадровых данных из ЕС. В отчете IAF рассмотрел связанные с трансграничной передачей данных риски для прав на защиту персональных данных (ст.8 Хартии Европейского союза по правам человека), а также риски для свободы профессиональной деятельности и права на труд (ст.15 Хартии).

## Если у европейского сервис-провайдера есть дочерняя компания в США, это то создает дополнительные риски?

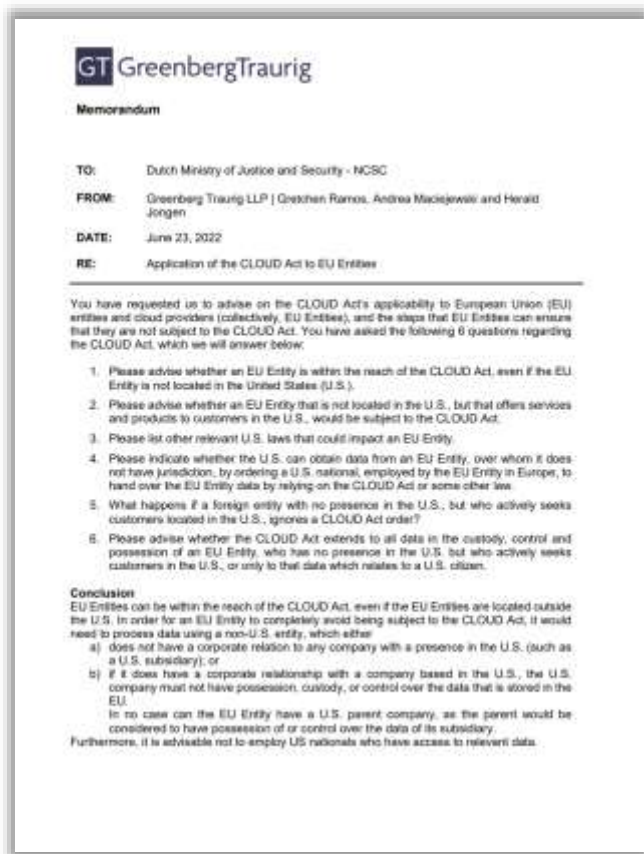


15.11.2021г. было опубликовано экспертное заключение профессора Stephen I. Vladeck из Школа права Техасского университета в Остине, подготовлено под эгидой Берлинского комиссара по защите данных и свободе информации от имени Конференции независимых надзорных органов по защите данных федерального правительства и земель (Конференция по защите данных).

That said, the U.S. government has, in other contexts (*e.g.*, the Microsoft dispute that led to the CLOUD Act), taken the position that the only relevant consideration is whether the data is in the possession or control of a U.S. communication service provider as defined in 50 U.S.C. § 1881(b)(4). So an EU company with a U.S. subsidiary could well be subject to the section 702 regime, again because of the definition in § 1881(b)(4) includes “agents” of qualifying electronic communications service providers.

Thus, there's no clear, categorical answer to this question. Insofar as the data is at rest on U.S. servers or transiting through U.S. infrastructure, it can be subject to collection under section 702 regardless of where the *company* is that owns the servers and/or the infrastructure. Indeed, if a EU company has a U.S. subsidiary (or itself has a legal presence in the United States), the coercive sanctions discussed above could easily be used to compel compliance with directives under section 702. And insofar as the data is at rest on non-U.S. servers or transiting through non-U.S. infrastructure over which no U.S. company has *any* control, section 702 seems less squarely on point depending upon whether any U.S. company *could* exercise control.

## CLLOUD Act, наряду с FISA 702 и EA 12333, должен быть проанализирован в TIA по передаче данных в США



Министерство юстиции и безопасности Нидерландов опубликовало исследование, которое они получили от американской юридической фирмы в отношении американского Закона CLOUD.

Предоставление данных в соответствии с Законом CLOUD применяется даже к дочерним компаниям ЕС материнских компаний США. Это придает больший вес риску того, что при рассмотрении вопроса о применимости главы V контролеры должны также проверить, имеет ли контрагент из ЕС материнскую компанию из США.

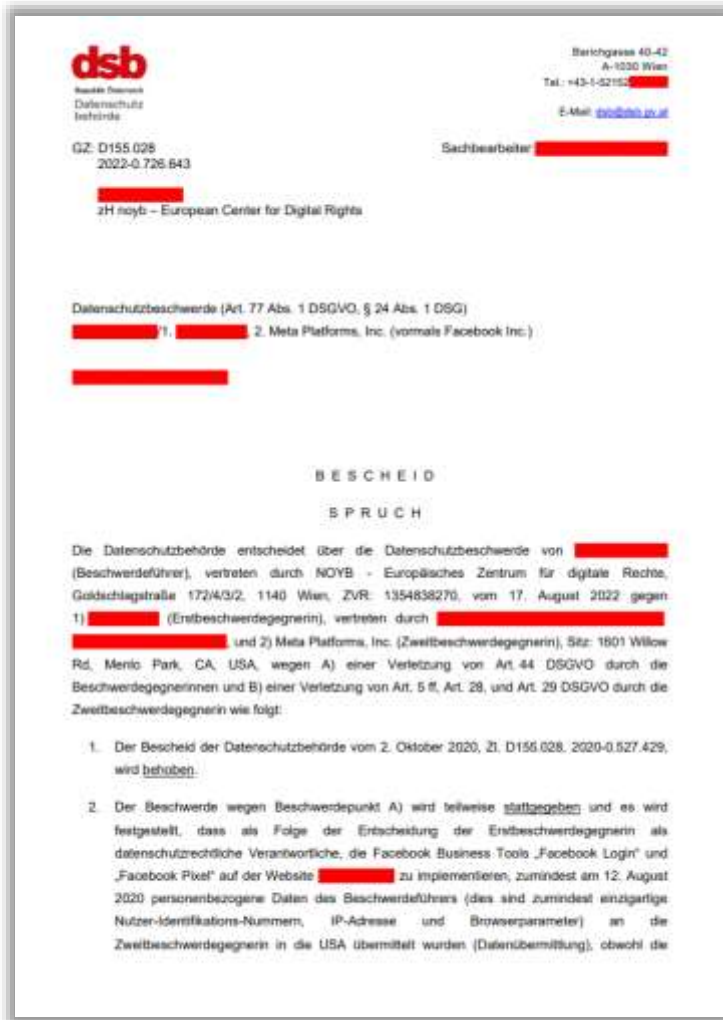
Компания из ЕС может подпадать под действие CLOUD Act напрямую, если она удовлетворяет правилам США о юрисдикции (тест на минимальные контакты). Компаниям может потребоваться полностью заблокировать запросы с IP-адресов США или, по крайней мере, разместить уведомление о том, что веб-сайт не предназначен для использования лицами из США. В противном случае США могут запросить доступ непосредственно у организации ЕС.

Другой областью угроз являются физические лица, работающие в компаниях ЕС. Если правительство США обладает юрисдикцией над ними, оно может опираться на закон CLOUD. Оно также может применить более простые средства, такие как запрос на добровольное предоставление информации, повестка в суд и т.д.

У компании из ЕС есть возможность оспорить запрос закона CLOUD на основании (1) «принципа вежливости» общего права, который позволяет оспаривать ордера, если они создают конфликт с иностранным законодательством; или (2) на основании нормативной базы закона CLOUD, регулирующей конфликты с иностранным законодательством.

Таким образом, это еще один шаг к запрету работы с американскими дочерними компаниями, принадлежащими ЕС.

## Австрийский DSB о том, что web-пиксели Meta нарушают решение CJEU по делу Schrems II



Австрийский орган по защите данных ("DSB") 06.03.2023 вынес решение о том, что web-пиксель для отслеживания действий пользователей Meta Platforms, Inc (ранее Facebook Inc.) нарушает GDPR и решение Суда Европейского союза ("CJEU") по делу «Schrems II».

Это решение является результатом 101 жалобы, поданной НКО "Не ваше дело" ("NOYB") ранее и определяет, что незаконность Google Analytics также распространяется на инструменты Facebook Login и Meta Pixel, предоставляемые компанией Meta. DSB заключило, что данные неминуемо передаются в США, где они подвергаются риску доступа со стороны американских спецслужб.



## Палата по государственным закупкам Баден-Вюртемберг решила, что возможный трансграничный доступ к данным нарушает главу V GDPR

Палата государственных закупок земли Баден-Вюртемберг 13.07.2022 вынесла решение о том, что американские поставщики цифровых серверов и/или облачных услуг не могут законно предоставлять свои услуги через европейские дочерние компании в свете решения Суда Европейского Союза ("CJEU") по делу Schrems II, несмотря на использование стандартных договорных оговорок ("SCC").

Вопрос возник в контексте тендера на закупку программного обеспечения для цифровых услуг, в ходе которого проигравший участник оспаривал присуждение контракта выигравшему участнику из-за его несоблюдения главы V GDPR. В связи с этим проигравший участник торгов потребовал пересмотра заявки и исключения выигравшей стороны из процедуры оценки.

Палата рассмотрела конкурсное предложение и отметила, что нарушения защиты данных, в которых обвинили победившего участника торгов, касались ст.44 и иных норм GDPR, поскольку участник торгов обрабатывал персональные данные на серверах, к которым могли иметь доступ третьи страны (в частности, США), и что проигравший участник торгов утверждал, что возможность такого доступа представляет собой обработку данных, то есть передачу данных в смысле ст.44 GDPR.

В связи с этим палата установила, что передача персональных данных в третью страну является незаконной в соответствии с законодательством о защите данных, если соответствующий сервер эксплуатируется компанией, расположенной в ЕС, которая также является частью американской группы. Таким образом, палата постановила, что "простая возможность" того, что к персональным данным может получить доступ материнская компания из США, приводит к передаче по смыслу GDPR, независимо от того, получает ли материнская компания из США фактический доступ к персональным данным.

**07.09.2022 Высший региональный суд Карлсруэ (Oberlandesgericht Karlsruhe) отменил решение VG Baden Württemberg. OLG Karlsruhe рассудил, что суды, выносящие решения в отношении участников процесса закупок, не могут отказать участнику торгов только на основании предположения, что участник торгов или его субпроцессоры нарушат свои собственные договорные обязательства по хранению данных в ЕС в случае запроса доступа со стороны властей США.**

## EDPS признал Еврокомиссию нарушителем GDPR из-за использования облачных сервисов Microsoft 365

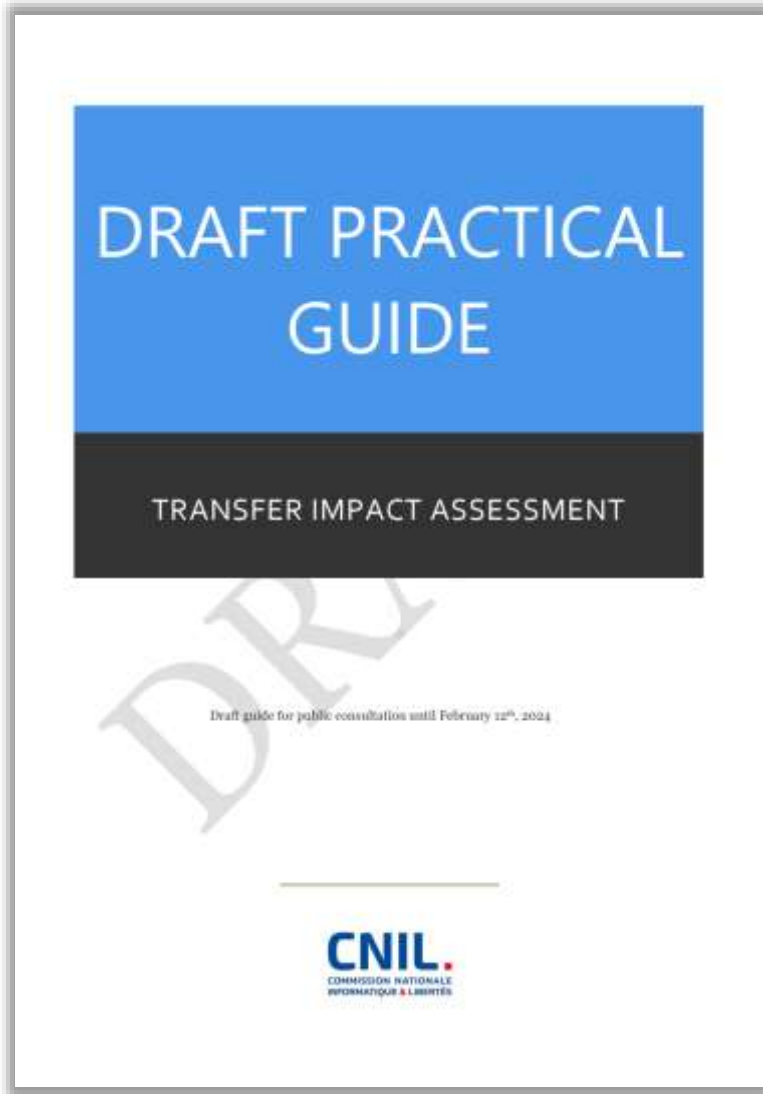


Использование Еврокомиссией (ЕК) программного обеспечения (ПО) Microsoft нарушает нормы GDPR, кроме того, ЕК не смогла внедрить «адекватные защитные механизмы» для ПД, передаваемых в государства за пределы Евросоюза, сообщил 11.03.2024 Европейский надзорный орган по защите данных (European Data Protection Supervisor, EDPS).

В этой связи EDPS предписал ЕК предпринять меры для соблюдения законодательства и прекратить передачу данных американской компании и её «дочкам» в третьи страны, с которыми у ЕС нет соглашений об охране ПД. Срок для выполнения предписаний — 09.12.2024.

«В контракте с Microsoft Еврокомиссия должным образом не уточнила, какие типы ПД будут собраны и для каких конкретно целей при использовании Microsoft 365», – пояснили в EDPS.

## 579 Руководство французского CNIL по Transfer Impact Assessment (TIA)



Французский орган по защите данных (CNIL) опубликовал текст практического руководства по оценке воздействия на передачу данных (TIA), которое включает в себя методологию и контрольный список, в котором указаны различные элементы, которые необходимо учитывать при проведении TIA.

Руководство содержит указания на то, как можно провести анализ, следуя шести этапам, изложенным в рекомендациях EDPB, и указывает на соответствующую документацию. Также отмечается, что руководство не является оценкой законов и практики в третьей стране и связанных с ними рисков.

# FAQ от Давида Розенталя по новым EU Standard Contractual Clauses и Transfer Impact Assessment (TIA)

VISCHER

Version of 21-08-01

## FREQUENTLY ASKED QUESTIONS (FAQ)

### NEW EU STANDARD CONTRACTUAL CLAUSES FOR DATA TRANSFERS TO NON-WHITELISTED THIRD COUNTRIES

taking into account the version 2.0 of the EDPB's recommendation 01/2020

By David Rosenthal, VISCHER AG\* (translated from German<sup>1</sup>)

The following questions relate to the standard contractual clauses for data transfers to third countries (SCCs) adopted by the European Commission on June 4, 2021, i.e. within the meaning of Art. 46 EU General Data Protection Regulation (GDPR). For the standard contractual clauses for processors (SCCs-DPA) see question 45. The commentary is based on the English version of the SCCs. Practical advice on the implementation of the new SCCs can be found in question 46. More information on the creation of an Intra-Group Data Transfer Agreement (IGDTA) (including an extensive checklist) is in question 47 and Transfer Impact Assessments (TIA) are addressed in question 42.

The Federal Data Protection and Information Commissioner (FDPIIC) has not yet commented on the validity and recognition of the SCCs under the Swiss Data Protection Act (CH DPA). This FAQ will be updated as soon as this happens.<sup>1</sup>

Version	Most important changes
June 22, 2021	First draft (English version only as a machine translation)
July 13, 2021	Manual translation, newly introduced question 8 (transfers to non-whitelisted third countries, if the importer is subject to the GDPR); clarifications on the meaning of "nature of processing" (question 19); the new question 21 (EU Member States); question 34 (sub-processor in Europe) and question 47 (IGDTA); more details on questions 41 and 42 (Schrems II and TIA) and the list of flaws in the SCC (question 43).
August 1, 2021	New question 7 (in which cases the EU SCC and TIAs are necessary); a new form for TIAs and further amendments concerning lawful access (questions 41 and 42); expansion of the IGDTA-Checklist (question 47)

Questions and feedback: [dataprivacy@vischer.com](mailto:dataprivacy@vischer.com)

1. What are the most important changes?..... 3
2. What risks does conclusion of the SCCs entail for the exporter and importer?..... 4

<sup>1</sup> Contributors: Samira Steiner, Mladen Stojkovic, Elias Flürger (all VISCHER), Maria Scharke to PHF Inc. (Pfalz/Wies), Christian Schreiber (Dreieck), Jörn Meier (DIA Riegel), David Szoska (Wald/Wies) and various others for their expert input to this FAQ. The author can be reached at [drosenthal@vischer.com](mailto:drosenthal@vischer.com).

<sup>2</sup> With the great support of Hanni Weder-Gillies (VISCHER); the original German master version is unofficially available here: <https://www.rosenthal.ch/downloads/VISCHER-faq-scc-en.pdf>.

<sup>3</sup> Unofficial permalink: <https://www.rosenthal.ch/downloads/VISCHER-faq-scc-en.pdf>.

VISCHER IGDTA.

Applies EU SCC in all official and unofficial transfer scenarios

Smoothly replace existing IGDTA, special solution for UK

Sign with only two parties, have others follow later

Definitions

Covers C-C and C-P transfers within EEA and whitelisted countries

List of parties, incl. supervisory authorities

Joint controllership and transfers within a company (e.g. HQ and branches)

Works smoothly, amendments, information flow, form, new parties, representatives, etc.

Detailed "catch all" description of data transfers, not only activities, all transfers allocated to parties

More detailed TDMS, for internal use and with third party providers

Joint Controller Agreement as per Art. 26 GDPR, including default allocation of responsibilities

EU SCC (in A/E)

Risk-based Transfer Impact Assessments, including an automated form (Excel)

Use affiliates as Art. 27 GDPR representatives (Appointment form)

New parties can join at any time (replaces EU SCC docking clause)

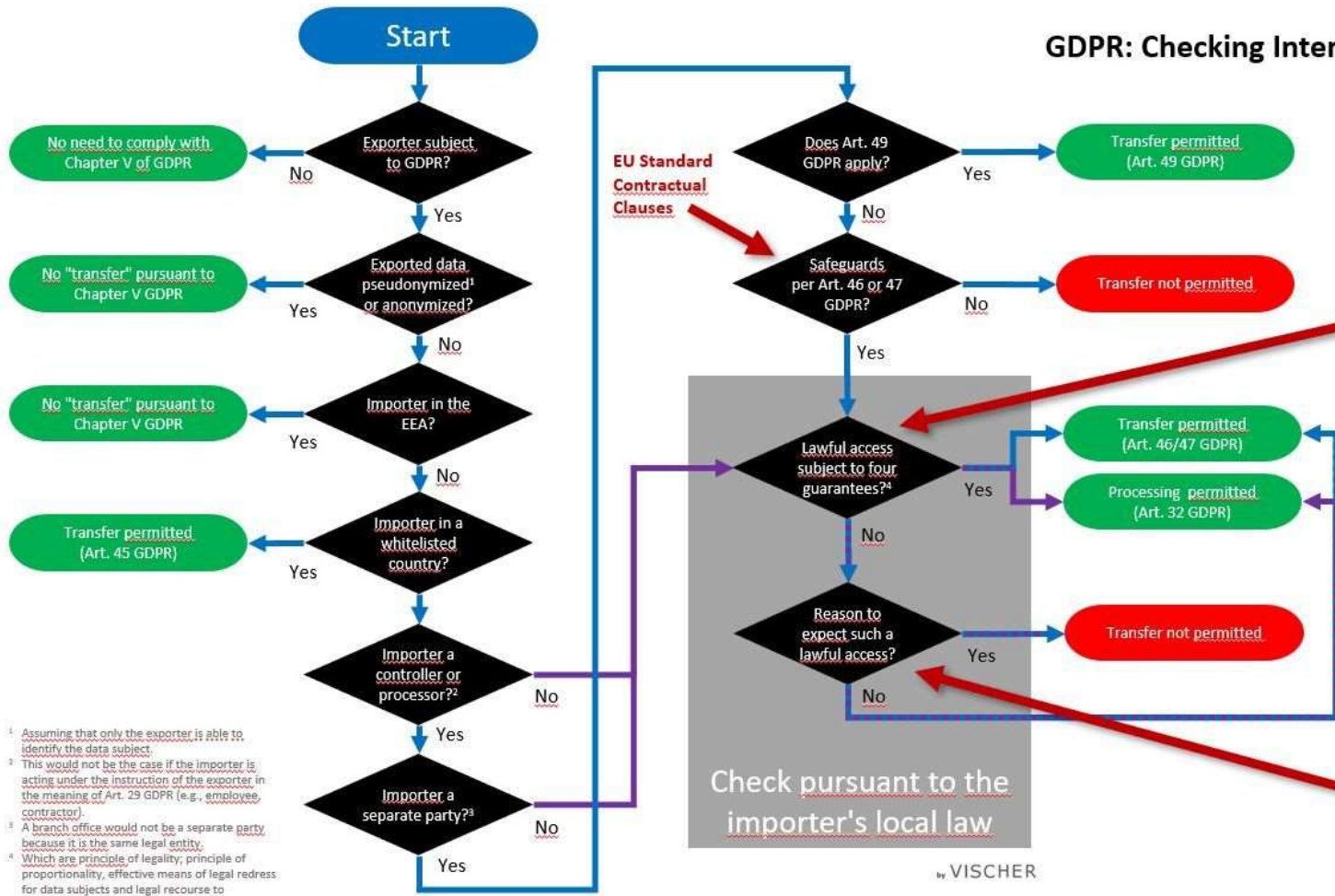
Sub-processors, with sample text

<http://rosenthal.ch/>

<https://www.rosenthal.ch/downloads/VISCHER-faq-scc-en.pdf>

<https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf>

# 581 Блок-схема применения ТИА от Давида Розенталя



## GDPR: Checking International Data Transfers



[https://www.rosenthal.ch/downloads/Rosenthal\\_Assessing\\_Lawful\\_Access\\_Laws.xlsx](https://www.rosenthal.ch/downloads/Rosenthal_Assessing_Lawful_Access_Laws.xlsx)  
<https://bit.ly/3JzKzd5>



[https://www.rosenthal.ch/downloads/Rosenthal\\_EU-SCC-TIA.xlsx](https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx)  
<https://bit.ly/3JnM4Lb>

Check pursuant to the importer's local law

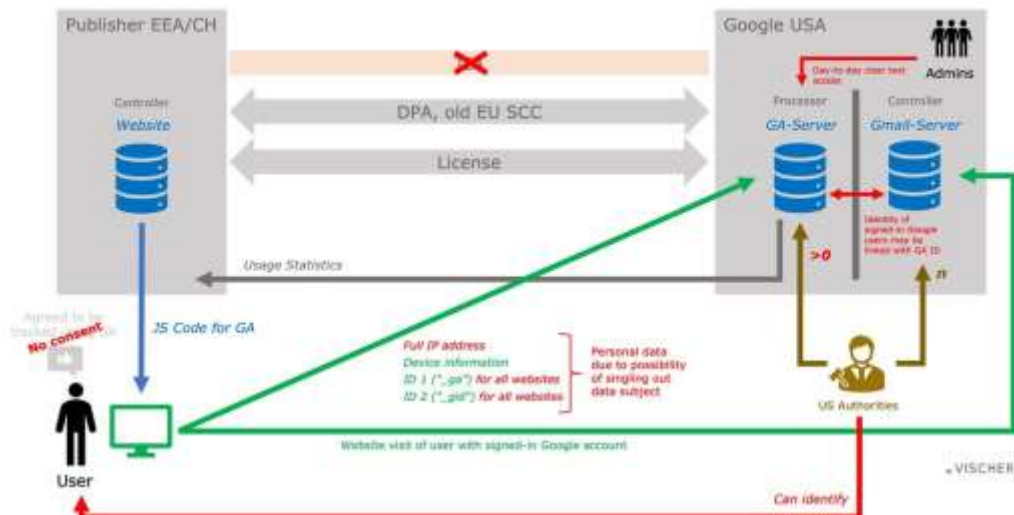
by VISCHER

TIA = Transfer Impact Assessment

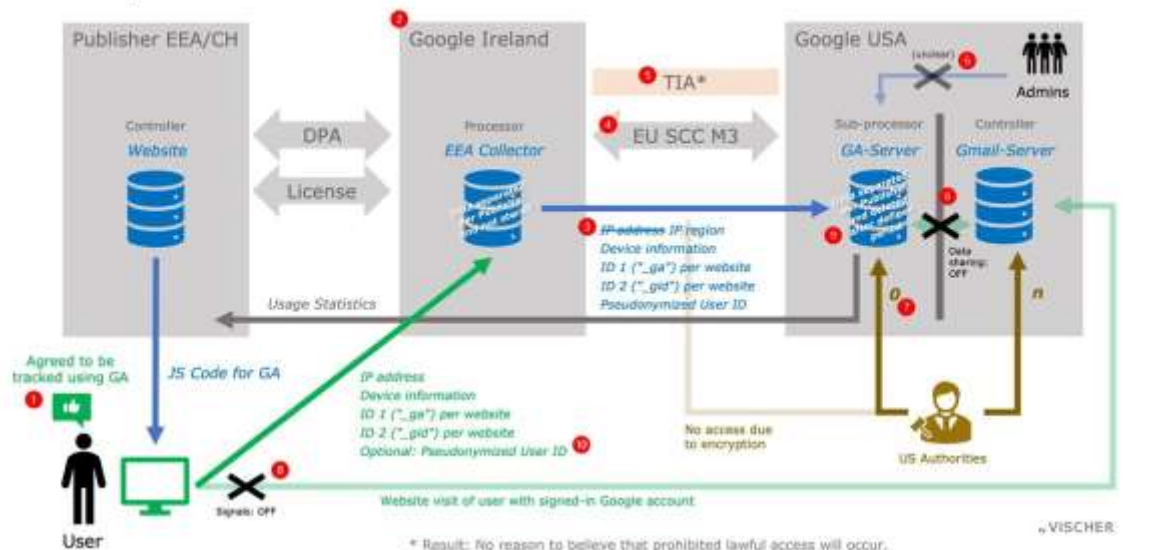
<sup>1</sup> Assuming that only the exporter is able to identify the data subject.  
<sup>2</sup> This would not be the case if the importer is acting under the instruction of the exporter in the meaning of Art. 29 GDPR (e.g., employee, contractor).  
<sup>3</sup> A branch office would not be a separate party because it is the same legal entity.  
<sup>4</sup> Which are principle of legality, principle of proportionality, effective means of legal redress for data subjects and legal recourse to independent and impartial body.

# Мнение Давида Розенталя о возможности легально использовать Google Analytics в ЕС/ЕЭЗ

Google Analytics (as assessed in the Austrian case)



Google Analytics (new setup, client-side mode)



# Пример ТІА от Давида Розенталя в отношении Amazon EC2, Amazon S3, and Amazon RDS

## Step 6: Data subject risks

- a) *Estimated probability of occurrence of successful lawful access risk:* 0,00% Very Low **Rationale**
  - b) *Estimated impact of risk:* 3= regular personal data in the clear High
- The Content Data can include special categories of data. Organisations are advised to apply their own encryption to such sensitive and special categories of data unless the data are already public (such as court hearings). The risk is low in 3 circumstances: (1) if the European Commission adopts a new adequacy decision for the USA (2) if organisations do not store such special categories of data in AWS's services, or if they do, absent an adequacy decision (3) they can control the key (and they use pseudonyms for employee admins whose identity should remain confidential)*

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

## Step 7: Define the safeguards in place

- a) Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead? Yes *Describe why you still do not pursue this option* **Rationale**
- b) Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)? No
- c) Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)? No *Ensure that data remains encrypted*
- d) Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)? Yes *Foreign lawful access is at least technically possible*
- e) Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)? Yes *Ensure that the mechanism remains in place and is complied with*

Based on the answers given above, the transfer is: permitted

*Absent a new adequacy decision from the EU for the USA, admins should apply encryption to Content Data with a self-controlled key if they want to use AWS to store sensitive and special categories of data.*

## CHECKLIST

## Transfer Impact Assessment (TIA) Checklist

The data transfer landscape has changed markedly since the CJEU's judgment in the Schrems II case. The decision invalidated the EU-US Privacy Shield and cast doubt over the effectiveness of the European Commission's existing Standard Contractual Clauses (SCCs).

In the fallout from the decision, the European Commission issued a revised set of SCCs for organizations to utilize and the European Data Protection Board (EDPB) released their finalized guidance on supplementary measures for ensuring an EU level of data protection when transferring personal data.

As part of their guidance, the EDPB highlighted the need for organizations to perform a Transfer Impact Assessment (TIA) to evaluate the Article 46 transfer tool in light of the legal framework and practical application of the law in the destination country.

This checklist will provide an overview of the key steps you can take as you perform a TIA as well as some key considerations your organization should keep in mind when assessing the legal frameworks for third countries.

### Understand the transfer

- Consult EDPB Supplementary Measures Recommendations Guidance

### Data importer

- Who is the data importer?
- What service does the data importer provide?
- What are the processing activities the data importer performs on your behalf?

### Know your data

- What categories of personal data are being transferred? (e.g., personal data of children, special categories of personal data/sensitive personal data).
- Will the data be stored in the third country or can data stored within the EU/EEA be remotely accessed?
- Is the data plain text, pseudonymised, or encrypted?

### Context of the transfer

- Which Article 46 transfer mechanism under Article 46 GDPR is being relied upon?
- Is the data being transferred subject to onward transfers from the third country to another third country?
- Is the transfer adequate, relevant, and limited to what is necessary?
- Does the data importer engage subprocessors to perform specific processing activities?
- Does the data importer rely upon appropriate safeguards or a derogation?

onetrust

## CHECKLIST

### Third country assessment

- Is the principle of the rule of law provided in the third country legal system?
- Does the third country respect human rights and fundamental freedoms?
- Is there a comprehensive data protection/privacy law?
- Do the appropriate legal remedies exist for data subjects to exercise their rights?
- Does the third country's data protection system contain safeguards for special categories of personal data?
- Does the third country have public security, defence, national security, and/or criminal laws that enable public authorities or law enforcement to access the transferred personal data?
- Has an independent supervisory authority been established in the third country?
- Has the third country entered into any legally binding conventions or instruments? (e.g., Convention 108)

### European Essential Guarantees

- Does the legal framework in the third country govern access to personal data by public authorities?
- Is the potential processing by public authorities based on clear, precise, and accessible rules?
- Are the legitimate objectives pursued by public authorities necessary and proportionate?
- Does an independent oversight mechanism exist?
- Is public authority interference subject to an effective, independent, and impartial oversight system that is provided for by a judge or another independent body?
- Is the independent oversight mechanism binding on the public authority?
- Do individuals have effective legal remedies to satisfy their rights before a tribunal?
- Does the law require notification to affected individuals of the surveillance measures in order to allow them to exercise their rights?
- Are effective remedies or rights to redress available to individuals whose personal data is processed by public authorities in the third country?

onetrust



## Анализ законодательства стран на предмет «адекватности» защиты данных с точки зрения требований ЕС

Filter:  Assessment available  EU Adequacy  CoE 108+ Ratifier

Country	Adequacy Decision European Commission	Adequacy Decision Switzerland	Adequacy Decision Monaco	Adequacy Decision Roskomnadzor, («адекватную защиту»)	CoE 108 Data Protection (Signed; (R)atified; (E)ntered into force	CoE 108+ (223) Data Protection (Signed; (R)atified; (E)ntered into force
+ Switzerland	✓ <a href="#">See here</a>	✓	✓	✓	S, R, E: 01/02/1998	S
+ Albania	✗	✗	✗	✓	S, R, E: 01/06/2005	
+ Bosnia and Herzegovina	✗	✗	✗	✓	S, R, E: 01/07/2006	S
+ Bahrain	✗	✗	✗	✗		
+ Georgia	✗	✗	✗	✓	S, R, E: 01/04/2006	
+ Hong Kong	✗	✗	✗	✗		
+ Japan	✓ <a href="#">See here</a>	✗	✗	✓ <a href="#">See here</a> or <a href="#">here</a>		
+ Kuwait	✗	✗	✗	✗		
+ Oman	✗	✗	✗	✗		
+ Qatar	✗	✗	✗	✓ <a href="#">See here</a> or <a href="#">here</a>		
+ Serbia	✗ <i>Potential future candidate (p. 52) for adequacy?</i>	✗	✗	✓	S, R, E: 01/01/2006	S, R
+ Russian Federation	✗	✗	✗	✓	S, R, E: 01/09/2013	S

# SCC Generator

CREATE YOUR OWN COPY OF THE NEW 2021 EU STANDARD CONTRACTUAL CLAUSES FOR PERSONAL DATA TRANSFERS TO THIRD COUNTRIES

## Information & Disclaimer

**Version 0.7 (beta)** Thank you for using the SCC Generator! This beta version was created by Christopher Schmidt, FIP CIPP/E CIPM CIPT CDPO/FR. The SCC Generator will be further developed!

Please share this tool and any feedback through [LinkedIn](#), [Twitter](#) or by **email**: [contribute@essentialguarantees.com](mailto:contribute@essentialguarantees.com)

All rights reserved. Information and materials on this web site are not legal advice. You should not act upon the information on this web site without seeking advice from a qualified lawyer licensed in your own country.

### Step 1: Select the Applicable Modules and Options for your SCCs

(Changes you make appear in real time below):

- Include MODULE ONE (C2C)
- Include MODULE TWO (C2P)
- Include MODULE THREE (P2P)
- Include MODULE FOUR (P2C)

Clause 7: Include Docking Clause (optional)?

Clause 11: Include right to lodge a complaint with an independent dispute resolution body?

RESET ALL SETTINGS

# Bird & Bird

## EU Standard Contractual Clauses Generator

If you would like to explore a bespoke version of this tool for your organisation(s) or have any question or feedback regarding our EU SCC generator, feel free to contact us at [scc@twobirds.com](mailto:scc@twobirds.com)

[Terms of use](#) - [Legal Notices](#) - [Privacy](#)

Please select one of the following options regarding the relationship:

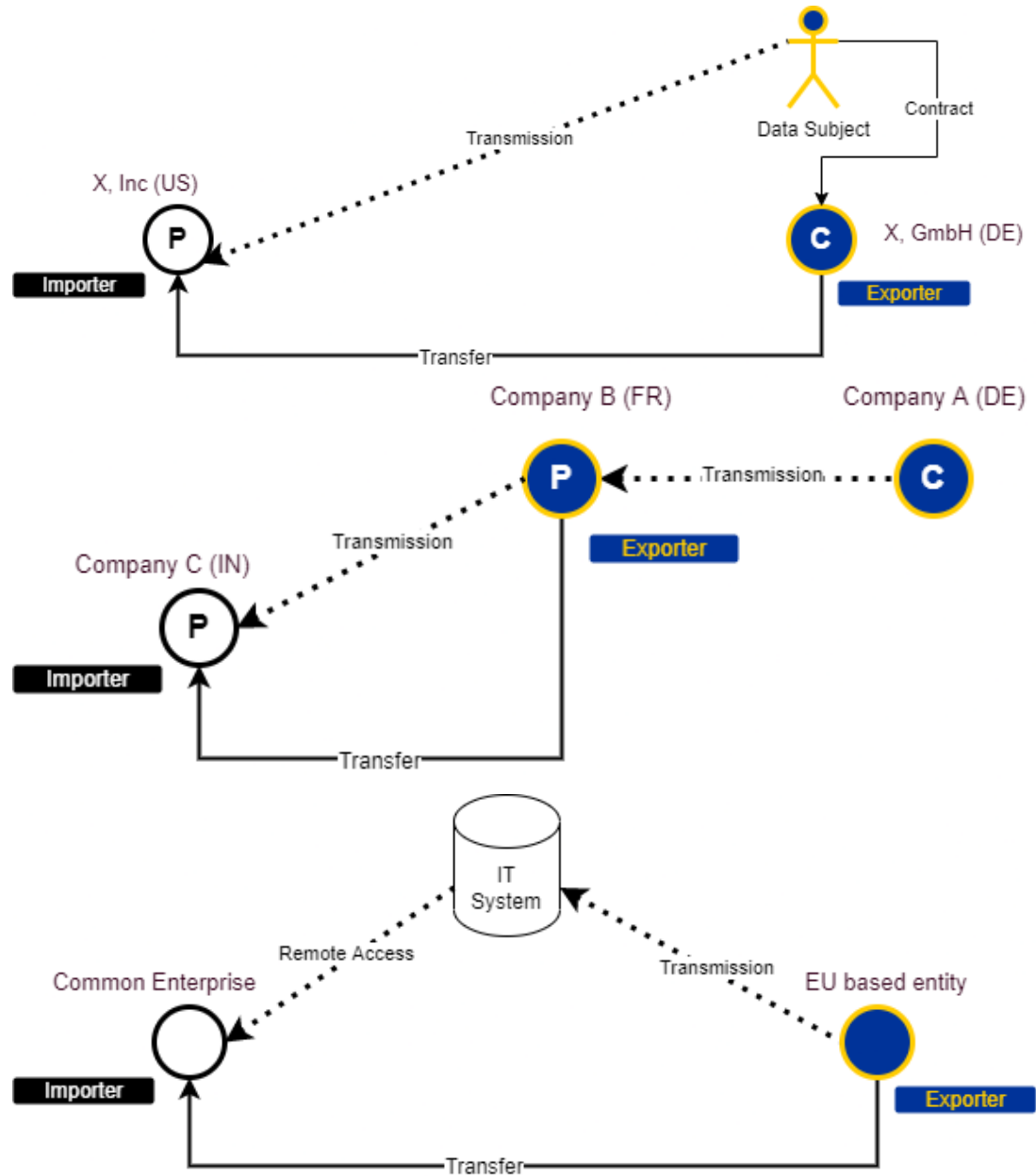
- Controller to Controller (Module 1)
- Controller to Processor (Module 2)
- Processor to Processor (Module 3)
- Processor to Controller (Module 4)

## 588 Трансграничная передача данных в диаграммах




### Privacy Maverick

Privacy provocateur. Digital nomad.




## 589 Понятие международной передачи данных: о чем вам не рассказал EDPB

DPOrganizer



BLOG POST

### The notion of international data transfers: what the EDPB did not tell you

 KONSTANTIN TIAZHELNIKOV

AUGUST 10, 2022 - 9 MIN READ

The GDPR itself, paired with multiple Recommendations and Guidelines issued by the European Data Protection Board (EDPB) and supplemented with the decisions of the CJEU and the EEA national supervisory authorities, contains intricate provisions on what is called "a transfer of personal data to a third country or international organisation".

To get an understanding of when special data transfer rules apply, it is crucial to figure out what is hidden behind the wording "a transfer of personal data to a third country or international organisation" (hereinafter – international data transfers).

- 1) Смешение двух подходов к характеру международной передачи данных.
- 2) Что на самом деле означает "данные раскрываются непосредственно субъектом данных и по его/ее инициативе"?
- 3) Определение понятий "экспортер данных" и "импортер данных".
- 4) Командировочные работники. Или внешние консультанты?
- 5) Что означает "географически в третьей стране"?

## Типовые договорные условия (МСС) Конвенции 108 для трансграничной передачи данных



Комитет Конвенции 108 (Т-РД) утвердил типовые договорные условия (МСС) для трансграничной передачи данных. Условия предназначены для трансграничной передачи персональных данных между двумя операторами в тех случаях, когда такая передача осуществляется в государство, не являющееся участником Конвенции 108 Совета Европы (СЕ) о персональных данных. Принятие условий в виде отдельного соглашения или дополнения к договору является мерой, способствующей достижению адекватного уровня защиты персональных данных, требуемого Конвенцией.

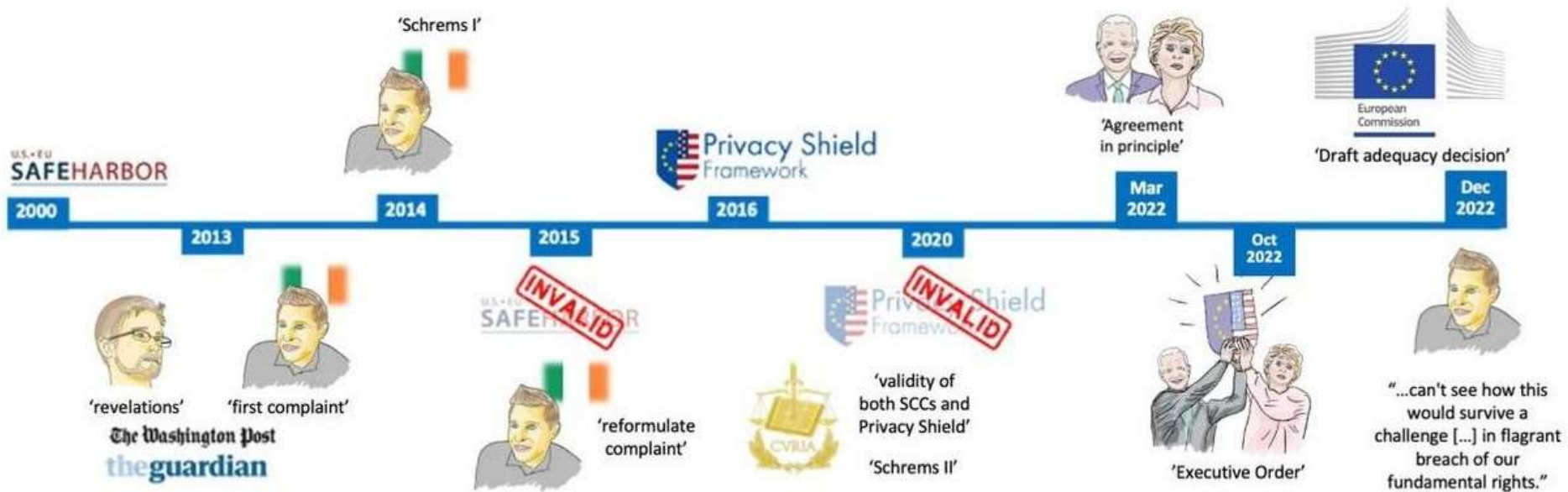
В отличие от аналогичного инструмента ЕС, имеющего прямое действие, типовые договорные условия СЕ должны быть одобрены национальным органом по надзору в сфере персональных данных государства, в юрисдикции которого находится оператор-экспортёр.

Комитет Конвенции также готовит к утверждению ещё два модуля, адресующего другие сценарии передачи данных, помимо сценария "от оператора к оператору".

# EU-US Data Privacy Framework



# Эволюция подходов ЕЭЗ к регулированию трансграничной передачи персональных данных в США





## Переговоры ЕС и США о Privacy Shield 2.0: Transatlantic Data Privacy Framework

### Key principles

- ◆ Based on the new framework, **data will be able to flow freely and safely** between the EU and participating U.S. companies
- ◆ A new set of rules and **binding safeguards to limit access to data** by U.S. intelligence authorities to what is **necessary and proportionate** to protect national security; U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
- ◆ **A new two-tier redress system** to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a **Data Protection Review Court**
- ◆ **Strong obligations for companies** processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce
- ◆ **Specific monitoring and review mechanisms**



### Benefits of the deal

- ◆ Adequate protection of Europeans' data transferred to the US, addressing the ruling of the European Court of Justice (*Schrems II*)
- ◆ Safe and secure data flows
- ◆ Durable and reliable legal basis
- ◆ Competitive digital economy and economic cooperation
- ◆ Continued data flows underpinning €900 billion in cross-border commerce every year



Next steps: The agreement in principle will now be translated into legal documents. The U.S. commitments will be included in an Executive Order that will form the basis of a draft adequacy decision by the Commission to put in place the new Trans-Atlantic Data Privacy Framework.



## 594 Белый дом опубликовал общие принципы передачи ПД европейцев в США

Президент США Джо Байден 07.10.2022 подписал исполнительный указ о повышенных гарантиях безопасности в рамках деятельности американской радиоэлектронной разведки; документ в том числе определяет общие принципы передачи персональных (ПД) европейцев в США.

Исполнительный указ определяет шаги, которые США «предпримут для выполнения обязательств в рамках договора об обеспечении конфиденциальности данных для обмена между Соединёнными Штатами и ЕС (European Union-U.S. Data Privacy Framework, DPF)».

Исполнительный указ:

- устанавливает дополнительные защитные механизмы для американской радиоэлектронной разведки, включая требование о том, что разведдеятельность ведётся исключительно для выполнения определённых задач, связанных с обеспечением национальной безопасности, с учётом права на личную жизнь и гражданских свобод всех лиц независимо от гражданства или страны проживания, ведётся исключительно тогда, «когда необходимо продвигать утверждённые приоритетные задачи разведки только в объёме и способами, пропорциональными этим задачам»;
- вводит требования по обработке ПД, собранных в результате деятельности радиоэлектронной разведки, и усиливает ответственность чиновников «для обеспечения надлежащих мер по выплате компенсации в случае нарушения требований»;
- создаёт «многоуровневый механизм» для физических лиц из установленных государств и региональных организаций по экономической интеграции для проведения независимого обязательного анализа и удовлетворения исков по поводу того, что ПД физлиц, собранные разведкой, были получены или обработаны США в нарушение американского законодательства, включая дополнительные защитные механизмы из данного исполнительного указа.

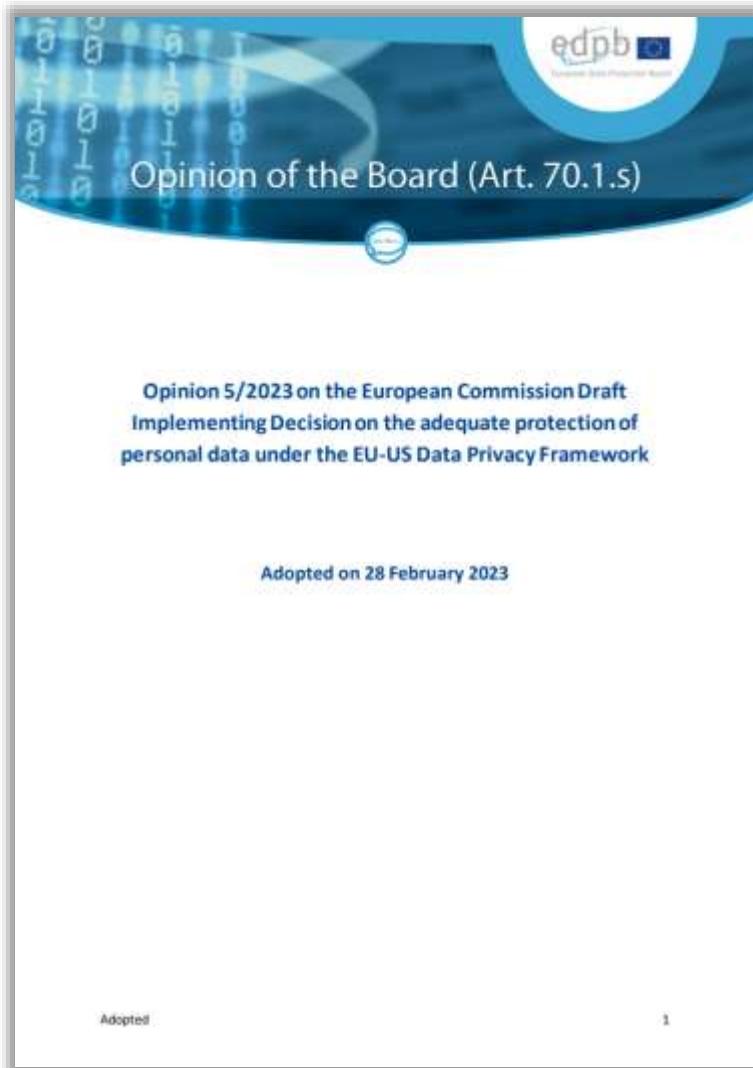
**Вместе с тем, ключевые эксперты в области регулирования ПД, например, Омер Тен, согласны с тем, что выбранный механизм предоставления гарантий — через Указ Президента США — вряд ли удовлетворит прайваси-активистов. Последние с самого начала отмечали, что для того, чтобы новые договоренности между США и ЕС устояли в Европейском суде справедливости, гарантии защиты прав граждан должны быть закреплены в законе, а не в более легко изменяемом акте органа исполнительной власти.**



13.12.2022 Европейская комиссия опубликовала проект решения об адекватности Рамочного соглашения о защите данных между ЕС и США (EU-US Data Privacy Framework), направленного на содействие безопасным потокам данных и решение проблем, возникших в связи с решением Суда Европейского союза (CJEU) по делу "Комиссар по защите данных против Facebook Ireland Limited, Максимилиан Шремс" (C-311/18) ("Дело Шремс II"). В частности, Комиссия пояснила, что проект решения о достаточности основан на ее оценке правовой базы США, которая включает в себя исполнительный указ, подписанный президентом Джо Байденом, а также нормативные акты, учреждающие Суд по рассмотрению вопросов защиты данных, и разрешает передачу персональных данных между ЕС и сертифицированными организациями в США.

Проект решения об адекватности был направлен в Европейский совет по защите данных ("EDPB"), на который EDPB 28.02.2023 предоставил [заключение](#) с рядом озабоченностей и рекомендаций. После этого Комиссия обратится за одобрением в комитет, состоящий из представителей государств-членов ЕС. Примечательно, что Европейский парламент также будет иметь право пересмотреть решение об адекватности. После завершения этой процедуры Комиссия сможет приступить к принятию окончательного решения об адекватности.

## 596 Озабоченность EDPB в отношении EU-US DPF



Европейский совет по защите данных (European Data Protection Board, EDPB) во вторник выразил озабоченность проектом нового соглашения о передаче персональных данных (ПД) между ЕС и США (European Union-U.S. Data Privacy Framework, DPF).

По мнению EDPB, ряд принципов нового соглашения не претерпел изменений по сравнению с действовавшим ранее договором, известным как «Щит конфиденциальности» (Privacy Shield). Ранее Суд Европейского Союза признал этот договор незаконным.

Озабоченность регулятора, в частности, связана с отсутствием ключевых определений, недостаточной ясностью требований к операторам ПД.



News  
European Parliament

Headlines Press room Agenda FAQ Election Press Kit

Press room / MEPs against greenlighting data transfers with the U.S. under current rules

## MEPs against greenlighting personal data transfers with the U.S. under current rules

Press Releases **LIBE** 13-04-2023 - 12:09

- EU citizens need legal certainty and a future-proof regime
- Rights to redress and access to information must be respected
- Current proposal likely to be invalidated by a court ruling, say MEPs

**The proposed EU-U.S. Data Privacy Framework is an improvement, but not enough to justify an adequacy decision on personal data transfers, say MEPs in a resolution.**

In a resolution adopted by Civil Liberties Committee MEPs on Thursday, MEPs argue that the European Commission should not grant the United States an adequacy decision deeming its level of personal data protection essentially equivalent to that of the EU and allowing for transfers of personal data between the EU and U.S.

According to the text, the EU-U.S. Data Privacy Framework is an improvement on previous frameworks, but does not provide for sufficient safeguards. MEPs note that the framework still allows for bulk collection of personal data in certain cases; does not make bulk data collection subject to independent prior authorisation, and does not provide for clear rules on data retention.

Комитет по гражданским свободам, юстиции и внутренним делам ("LIBE") Европейского парламента 13.04.2023 принял резолюцию об адекватности защиты, предоставляемой Рамочной программой ЕС-США по конфиденциальности данных (EU-US Data Privacy Framework), в котором делается вывод о том, что она не обеспечивает эквивалентную защиту. Проект предложения призывает Комиссию продолжить переговоры с США с целью создания механизма, который обеспечит такую эквивалентность и предоставит адекватный уровень защиты, требуемый законодательством ЕС о защите данных и Хартией основных прав ЕС в интерпретации CJEU.

Изложение принципов режима защиты данных ЕС в Исполнительном указе президента США не соответствуют практикам в ЕС и их толкованию Судом Европейского Союза (CJEU). Кроме того, в отношении Суда по рассмотрению вопросов защиты данных в США указано, что его решения будут засекречены, а сам суд будет частью исполнительной, а не судебной власти. При этом механизм возмещения ущерба не устанавливает обязательства уведомлять заявителя о том, что его персональные данные были обработаны. Таким образом, в проекте ходатайства утверждается, что такой суд подрывает право на доступ к персональным данным или их исправление.

## 598 Еврокомиссия утвердила EU-US DPF

Европейская комиссия 10.07.2023 утвердила EU-US Data Privacy Framework (DPF). Был сделан вывод о том, что США обеспечивают уровень защиты, по существу эквивалентный уровню ЕС, для персональных данных, передаваемых в соответствии с EU-US DPF от контроллера или процессора в ЕС сертифицированным организациям в США. Ntghtm передача персональных данных от контроллеров и процессоров в ЕС сертифицированным организациям в США может осуществляться без необходимости получения каких-либо дополнительных разрешений.

Положения EU-US DPF применяются сразу после сертификации получателя данных в США, который должен ежегодно подтверждать выполнение требований EU-US DPF. Для обеспечения адекватного уровня защиты данных на практике необходимо наличие в США независимого надзорного органа, наделенного полномочиями по контролю и обеспечению соблюдения правил защиты данных. Сертифицируемые организации должны находиться под юрисдикцией компетентных органов США - Федеральной торговой комиссии (FTC) и Министерства торговли (DoT), которые обладают необходимыми полномочиями по проведению расследований и правоприменению для обеспечения соблюдения норм EU-US DPF.

EU-US DPF предусматривает новые обязательные гарантии, призванные снять озабоченность, высказанную Европейским судом (CJEU). К ним относятся ограничения, обеспечивающие необходимость и соразмерность деятельности США в области радиотехнической разведки при достижении определенных целей национальной безопасности. Кроме того, создание в США Суда по рассмотрению вопросов защиты данных (Data Protection Review Court, DPRC) позволяет частным лицам в ЕС подавать жалобы на предполагаемое нарушение их частной жизни и гражданских свобод. При необходимости DPRC может предписать соответствующим спецслужбам принять меры по исправлению ситуации, включая удаление данных, прекращение их приобретения и изменение практики сбора. Организации, которые будут уличены в постоянном несоблюдении принципов, будут исключены из EU-US DPF и должны будут вернуть или удалить персональные данные, полученные из ЕС.

[https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf\\_en](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en)

[https://ec.europa.eu/commission/presscorner/detail/en/ganda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/en/ganda_23_3752)



В брошюре говорится о том, что передача данных несертифицированным компаниям в США требует соответствующих гарантий, таких как стандартные договорные оговорки (SCC) или обязательные корпоративные правила (BCR). Кроме того, субъекты данных ЕС могут подать жалобу в свой национальный орган по защите данных, чтобы воспользоваться новым механизмом правовой защиты, независимо от инструмента передачи, используемого для передачи персональных данных в США.



### Anwendungshinweise

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes  
und der Länder vom 4. September 2023<sup>1</sup>

#### Übermittlung personenbezogener Daten aus Europa an die USA

Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen  
Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework)  
vom 10. Juli 2023

Mit diesen Anwendungshinweisen sollen die wesentlichen Hintergründe und Inhalte des neuen Angemessenheitsbeschlusses der Europäischen Kommission zum Datenschutzrahmen EU-USA vom 10. Juli 2023<sup>2</sup> (EU-US Data Privacy Framework, abgekürzt: EU-US DPF) erläutert werden. Sie richten sich sowohl an Verantwortliche und Auftragsverarbeiter in Deutschland, die personenbezogene Daten an die USA übermitteln, als auch an betroffene Personen. Die Anwendungshinweise beleuchten insbesondere die Reichweite und den Anwendungsbereich der Neuregelung, den Einsatz alternativer Instrumente für Übermittlungen an die USA sowie Umfang und Durchsetzung von Rechten betroffener Personen gegenüber Stellen in den USA.

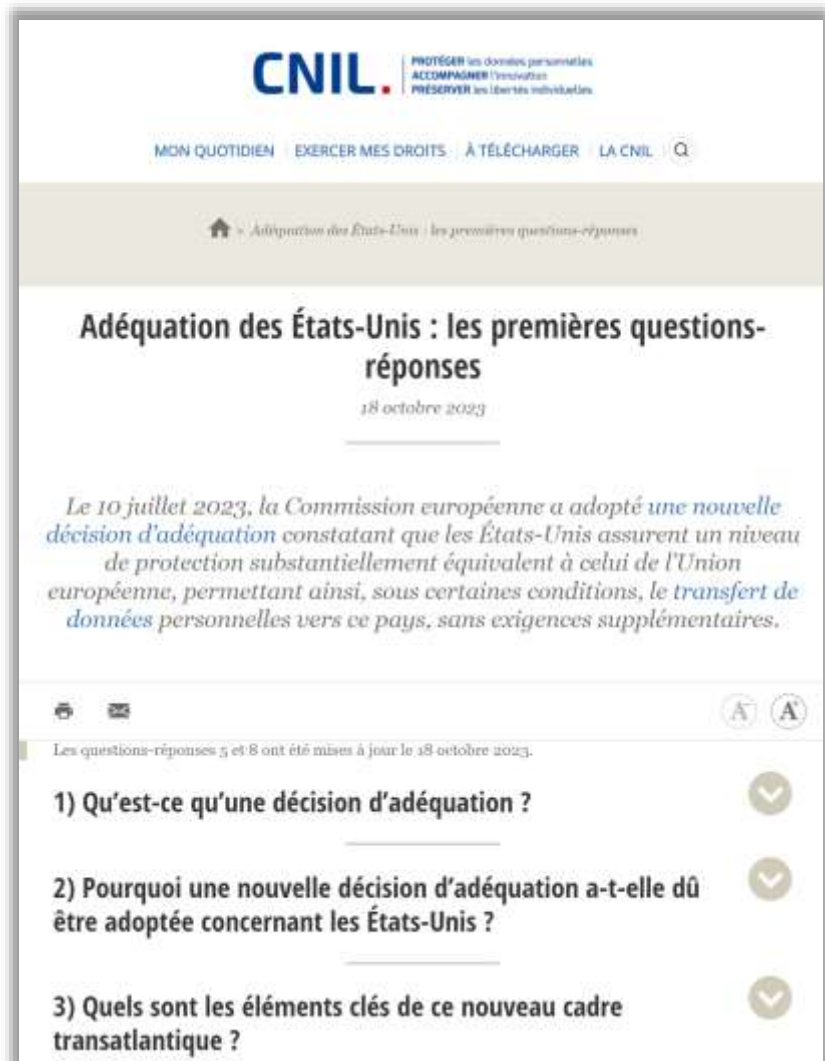
<sup>1</sup> Die Anwendungshinweise wurden durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit verabschiedet.

<sup>2</sup> Angemessenheitsbeschluss zum EU-US DPF, abrufbar unter:  
[https://commission.europa.eu/document/fa09cbad-d27d-4684-ae60-ba03f3b0f6df\\_en](https://commission.europa.eu/document/fa09cbad-d27d-4684-ae60-ba03f3b0f6df_en).

Немецкая конференция по защите данных (DSK) 04.09.2023 опубликовала свои разъяснения по применению решения Европейской комиссии о достаточности EU-US Data Privacy Framework (DPF) от 10.07.2023.

В документе описывается история создания, содержание, сфера применения и применение DPF, а также приводятся ссылки на многочисленные полезные материалы. Также указывается на возможность судебного пересмотра DPF Европейским судом (CJEU), однако отмечается, что на данный момент DPF применяется в соответствии с законодательством ЕС.



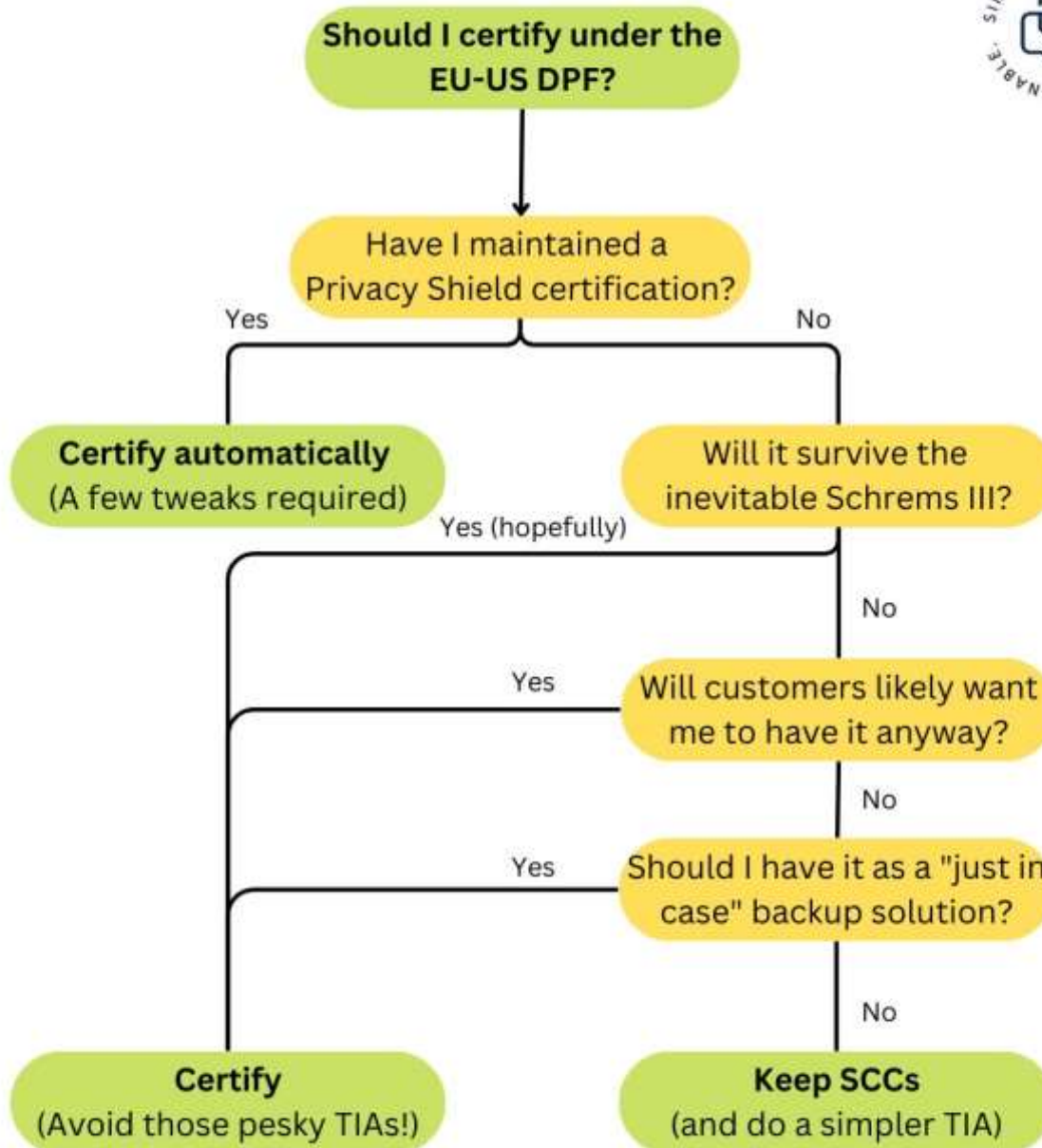


The screenshot shows the CNIL website header with the logo and tagline: "PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles". Navigation links include "MON QUOTIDIEN", "EXERCER MES DROITS", "À TÉLÉCHARGER", and "LA CNIL". The article title is "Adéquation des États-Unis : les premières questions-réponses" dated "18 octobre 2023". A summary text states: "Le 10 juillet 2023, la Commission européenne a adopté une nouvelle décision d'adéquation constatant que les États-Unis assurent un niveau de protection substantiellement équivalent à celui de l'Union européenne, permettant ainsi, sous certaines conditions, le transfert de données personnelles vers ce pays, sans exigences supplémentaires." Below the text are three numbered questions with expandable icons:

- 1) Qu'est-ce qu'une décision d'adéquation ?
- 2) Pourquoi une nouvelle décision d'adéquation a-t-elle dû être adoptée concernant les États-Unis ?
- 3) Quels sont les éléments clés de ce nouveau cadre transatlantique ?

Французский орган по защите данных (CNIL) 18.10.2023 опубликовал Q&A по поводу EU-US DPF в отношении исходящей из ЕС передачи персональных данных в США, в частности:

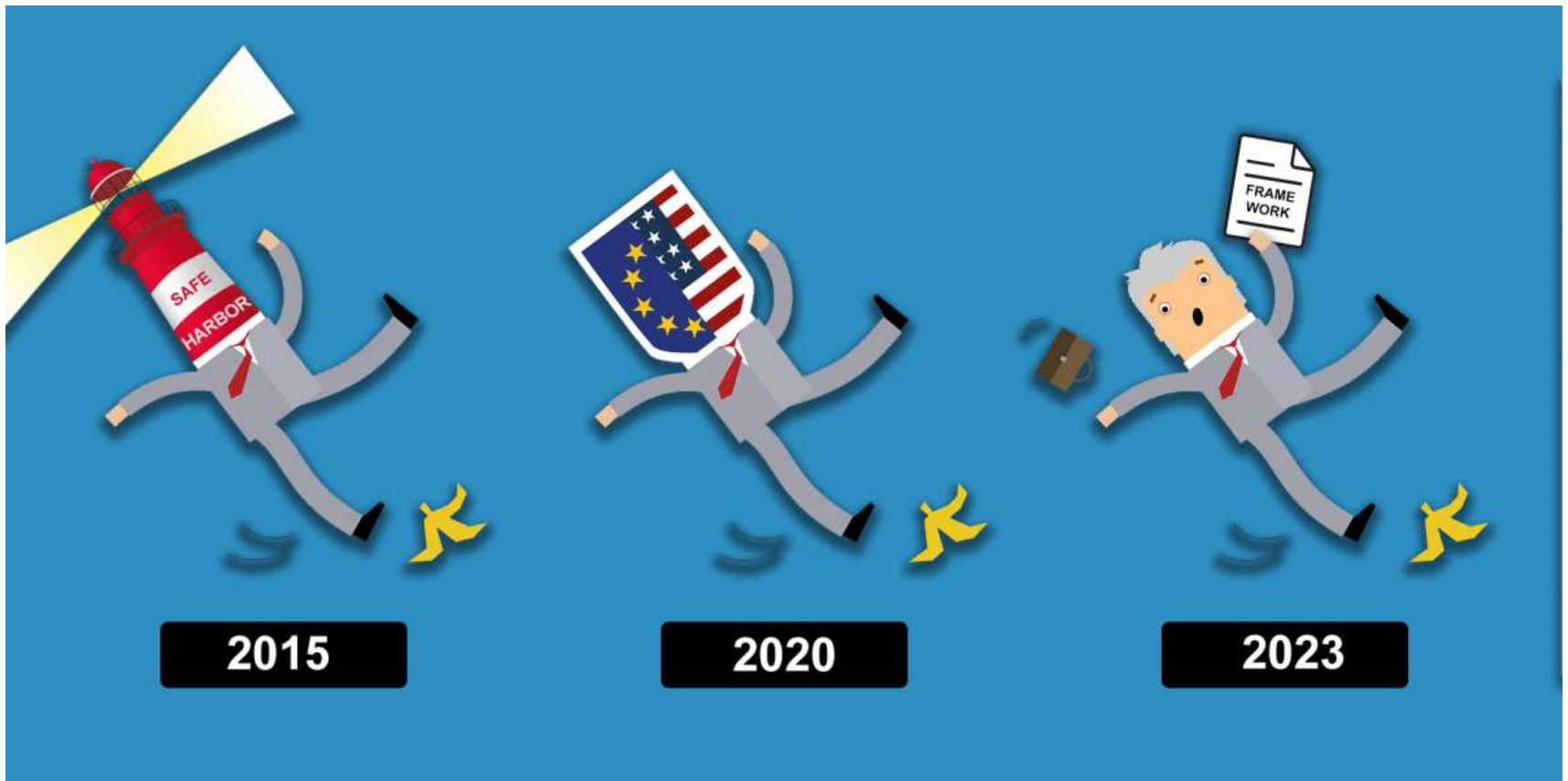
- что такое решение об адекватности(EU-US DPF)?
- почему необходимо принять новое решение об адекватности в отношении США?
- каковы ключевые элементы EU-US DPF?
- каковы последствия этого решения для организаций, желающих передавать данные в США?
- что должен предпринять контроллер данных, если организация-получатель не входит в список Министерства торговли США?
- каково влияние этого решения на организации, использующие другие инструменты передачи данных?
- могут ли администрации и местные органы власти воспользоваться этим решением в контексте передачи данных, связанной с использованием американских поставщиков услуг?
- когда решение об адекватности вступает в силу?
- как долго действует решение об адекватности?
- как будут рассматриваться жалобы, поданные в CNIL и касающиеся передачи данных в США, которая была осуществлена до принятия решения об адекватности?



## 603 На пути к «Шремс-III»: NOYB планирует оспорить EU-US DPF в CJEU

НКО «NOYB» планирует оспорить EU-US DPF в CJEU:

«Третья попытка Еврокомиссии добиться стабильного соглашения о передаче данных между ЕС и США, скорее всего, через несколько месяцев вновь окажется в Суде ЕС (CJEU). Предполагаемая "новая" Трансатлантическая структура конфиденциальности данных в значительной степени является копией неудавшегося "Щита конфиденциальности". Несмотря на пиар-акции Еврокомиссии, в законодательстве США и в подходе ЕС мало что изменилось. Фундаментальная проблема, связанная с FISA 702, не была решена в США, поскольку США по-прежнему придерживаются мнения, что только американские лица достойны конституционных прав.»



## Рекомендации, руководства и практические пособия



## 605 Руководства, рекомендации, лучшие практики от EDPB 1/2

[Руководства, рекомендации, лучшие практики](#) в области выполнения требований GDPR от Европейского совета по защите данных (European Data Protection Board):

1. [Guidelines 02/2023 on Technical Scope of Art. 5\(3\) of ePrivacy Directive](#)
2. [Guidelines 01/2023 on Article 37 Law Enforcement Directive](#)
3. [Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules \(Art. 47 GDPR\)](#)
4. [Guidelines 09/2022 on personal data breach notification under GDPR](#)
5. [Guidelines 08/2022 on identifying a controller or processor's lead supervisory authority](#)
6. [Guidelines 07/2022 on certification as a tool for transfers](#)
7. [Guidelines 06/2022 on the practical implementation of amicable settlements](#)
8. [Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement](#)
9. [Guidelines 04/2022 on the calculation of administrative fines under the GDPR](#)
10. [Guidelines 03/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them](#)
11. [Guidelines 02/2022 on the application of Article 60 GDPR](#)
12. [Guidelines 01/2022 on data subject rights - Right of access](#)
13. [Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR](#)
14. [Guidelines 04/2021 on Codes of Conduct as tools for transfers](#)
15. [Guidelines 03/2021 on the application of Article 65\(1\)\(a\) GDPR](#)
16. [Guidelines 02/2021 on virtual voice assistants](#)
17. [Guidelines 01/2021 on Examples regarding Personal Data Breach Notification](#)
18. [Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data](#)
19. [Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions](#)
20. [Guidance on certification criteria assessment \(Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation\)](#)
21. [Guidelines 10/2020 on restrictions under Article 23 GDPR](#)
22. [Recommendations 02/2020 on the European Essential Guarantees for surveillance measures](#)
23. [Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679](#)
24. [Guidelines 08/2020 on the targeting of social media users](#)

## 606 Руководства, рекомендации, лучшие практики от EDPB 2/2

24. [Guidelines 07/2020 on the concepts of controller and processor in the GDPR](#)
25. [Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR](#)
26. [Guidelines 05/2020 on consent under Regulation 2016/679](#)
27. [Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak](#)
28. [Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak](#)
29. [Guidelines 02/2020 on articles 46 \(2\) \(a\) and 46 \(3\) \(b\) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies](#)
30. [Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications](#)
31. [Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR \(part 1\)](#)
32. [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#)
33. [Guidelines 3/2019 on processing of personal data through video devices](#)
34. [Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment \(Article 39.4 of Regulation \(EU\) 2018/1725\)](#)
35. [Guidelines 2/2019 on the processing of personal data under Article 6\(1\)\(b\) GDPR in the context of the provision of online services to data subjects](#)
36. [Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679](#)
37. [Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation \(2016/679\)](#)
38. [Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\)](#)
39. [Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679](#)
40. [Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation](#)

[Письма](#) и иные значимые документы EDPB о выполнении требований GDPR:

1. [EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals](#)
2. [EDPB letter to ENISA regarding the European Cybersecurity Certification Scheme for Cloud Services \(EUCS\)](#)
3. [Statement on the processing of personal data in the context of the COVID-19 outbreak — 19/03/2020](#)
4. [EDPB Response to the MEP Sophie in't Veld's letter on unfair algorithms](#)
5. [Toolbox on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries](#)

## 607 Руководства, рекомендации, лучшие практики от WP29

Рекомендации Рабочей группы по защите физических лиц при обработке персональных данных ([Data Protection Working Party, WP29](#)), которая действовала до 25.05.2018. [Некоторые](#) из указанных рекомендаций продолжают действовать после расформирования Рабочей группы WP29 и передачи полномочий Европейскому совету по защите данных:

1. [Guidelines on consent under Regulation 2016/679, WP259 rev.01](#)
2. [Guidelines on transparency under Regulation 2016/679, WP260 rev.01](#)
3. [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01](#)
4. [Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01](#)
5. [Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01](#)
6. [Guidelines on Data Protection Officers \('DPO'\), WP243 rev.01](#)
7. [Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01](#)
8. [Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30\(5\) GDPR](#)
9. [Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, WP 263 rev.01](#)
10. [Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264](#)
11. [Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265](#)
12. [Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01](#)
13. [Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01](#)
14. [Adequacy Referential, WP 254 rev.01](#)
15. [Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253](#)

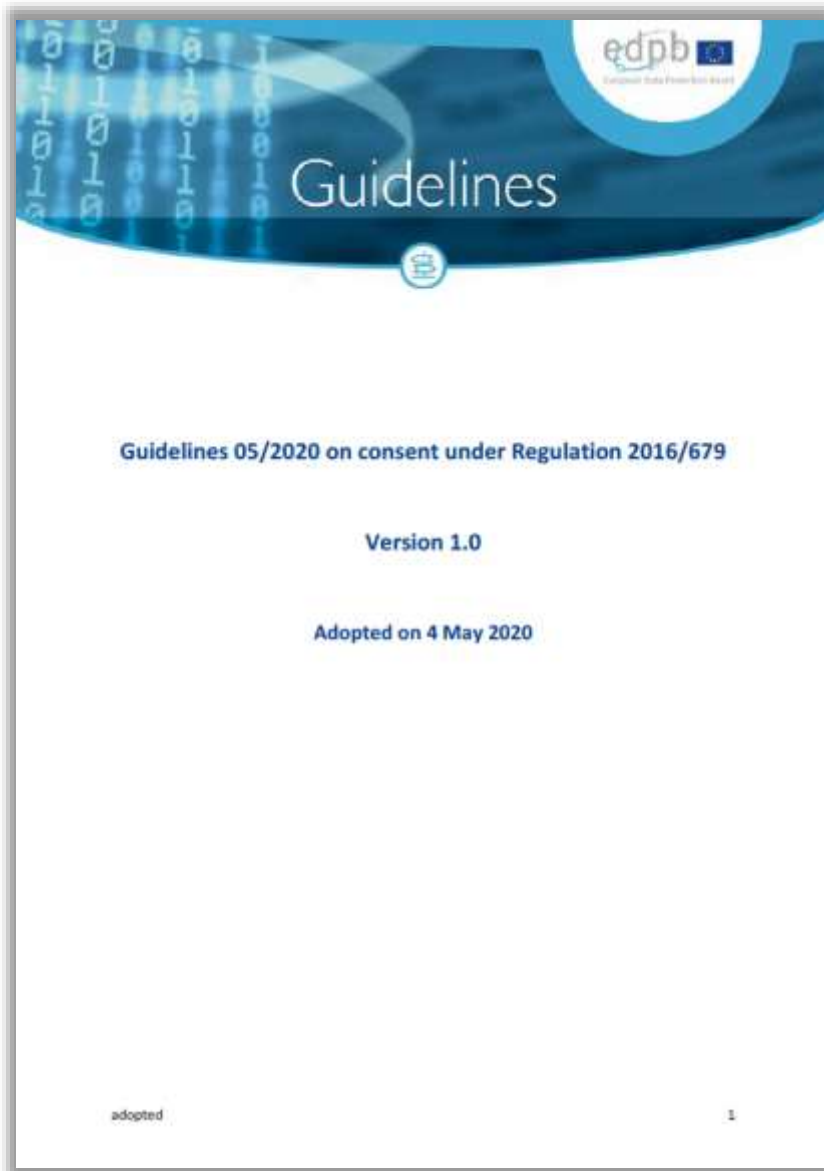
## 608 Мнения, отчеты, заявления и документы от WP29

Мнения, отчеты, заявления и документы Рабочей группы по защите физических лиц при обработке персональных данных ([Data Protection Working Party, WP29](#)), которая действовала до 25.05.2018:

1. [Opinion on Commission proposals on establishing a framework for interoperability - wp266](#)
2. [Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation \(2002/58/EC\) - wp247](#)
3. [Opinion on some key issues of the Law Enforcement Directive \(EU 2016/680\) - wp258](#)
4. [Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems \(C-ITS\) - wp252](#)
5. [Opinion 2/2017 on data processing at work - wp249](#)
6. [Opinion 03/2016 on the evaluation and review of the ePrivacy Directive wp240](#)
7. [Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain - wp179 update](#)
8. [Cookie sweep combined analysis, Report - wp229](#)
9. [Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes - wp230](#)
10. [Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones - wp231](#)
11. [Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing - wp232](#)
12. [Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes - wp234](#)
13. [Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - wp233](#)
14. [Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data \(European Essential Guarantees\) - wp237](#)
15. [Statement on the 2016 action plan for the implementation of the General Data Protection Regulation \(GDPR\) - wp236](#)
16. [Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision - wp238](#)
17. [Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector - wp239](#)
18. [Opinion 04/2016 on European Commission amendments proposals related to the powers of Data Protection Authorities in Standard Contractual Clauses and adequacy decisions - wp241](#)

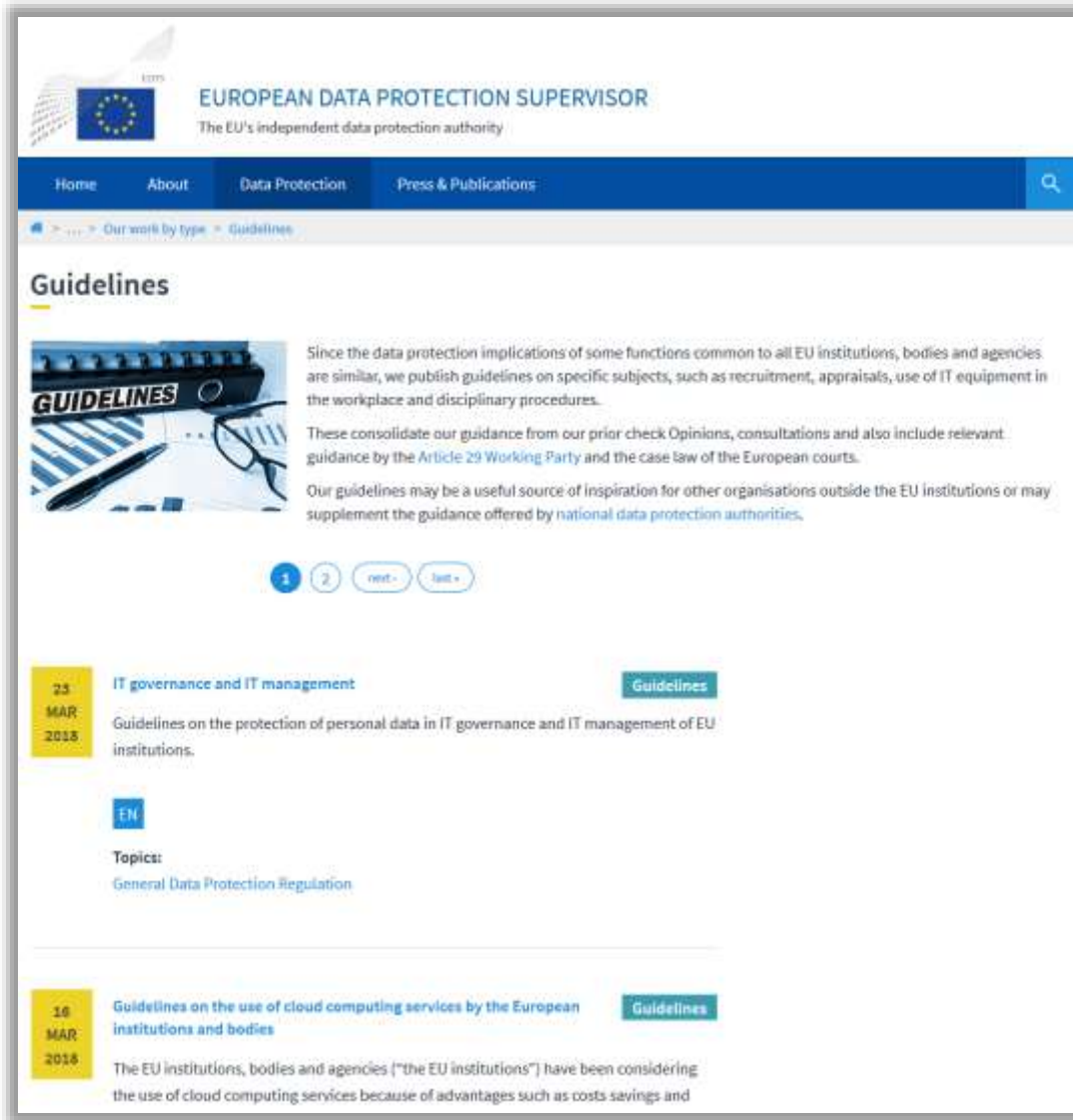


# Руководство EDPB о согласиях субъектов данных, получаемых в соответствии с GDPR



0	Preface.....
1	Introduction.....
2	Consent in Article 4(11) of the GDPR .....
3	Elements of valid consent .....
3.1	Free / freely given .....
3.1.1	Imbalance of power.....
3.1.2	Conditionality .....
3.1.3	Granularity.....
3.1.4	Detriment .....
3.2	Specific.....
3.3	Informed.....
3.3.1	Minimum content requirements for consent to be 'informed' .....
3.3.2	How to provide information.....
3.4	Unambiguous indication of wishes .....
4	Obtaining explicit consent.....
5	Additional conditions for obtaining valid consent .....
5.1	Demonstrate consent.....
5.2	Withdrawal of consent.....
6	Interaction between consent and other lawful grounds in Article 6 GDPR....
7	Specific areas of concern in the GDPR .....
7.1	Children (Article 8) .....
7.1.1	Information society service .....
7.1.2	Offered directly to a child.....
7.1.3	Age.....
7.1.4	Children's consent and parental responsibility .....
7.2	Scientific research .....
7.3	Data subject's rights .....
8	Consent obtained under Directive 95/46/EC.....

## 610 Рекомендации от EDPS



**EUROPEAN DATA PROTECTION SUPERVISOR**  
The EU's independent data protection authority

Home About Data Protection Press & Publications

Our work by type > Guidelines

### Guidelines

Since the data protection implications of some functions common to all EU institutions, bodies and agencies are similar, we publish guidelines on specific subjects, such as recruitment, appraisals, use of IT equipment in the workplace and disciplinary procedures.

These consolidate our guidance from our prior check Opinions, consultations and also include relevant guidance by the Article 29 Working Party and the case law of the European courts.

Our guidelines may be a useful source of inspiration for other organisations outside the EU institutions or may supplement the guidance offered by national data protection authorities.

1 2 next last

**23 MAR 2018** **IT governance and IT management** **Guidelines**  
Guidelines on the protection of personal data in IT governance and IT management of EU institutions.

**EN**  
**Topics:**  
General Data Protection Regulation

**16 MAR 2018** **Guidelines on the use of cloud computing services by the European institutions and bodies** **Guidelines**  
The EU institutions, bodies and agencies ("the EU institutions") have been considering the use of cloud computing services because of advantages such as costs savings and

Библиотека справочных материалов и рекомендаций в области обработки и защиты персональных данных от Европейского инспектора по защите данных (European Data Protection Supervisor), учитывающие актуальную правоприменительную и судебную практику ЕС.

The screenshot displays the Council of Europe's Data Protection website. The header includes the Council of Europe logo and the text "COUNCIL OF EUROPE" and "Data Protection". The navigation menu contains "Home", "Convention 108 and Protocols", "Activities", "Documentation", "Data Protection Commissioner", and "Data Protection Day". The breadcrumb trail reads "You are here: Data-protection > Documentation".

## Reports, studies and opinions

**2018** ^

- † T-PD(2018)01 The Practical Guide on the use of personal data in the police sector
- † T-PD(2018)05 Compilation of opinions
- † T-PD(2018)13rev Opinion on the Compatibility of the ICDDPPC Arrangement (including its schedule) with Convention 108+
- † Guidelines on Safeguarding Privacy in the Media
- † T-PD(2018)19 Opinion on the request for accession by the Republic of Kazakhstan

**2017** v

**2016** v

**2015** v

**2014** v


**2013** v

**2012** v

**2011** v

**2010** v

**2009** v

  
[www.coe.int/dataprotection](http://www.coe.int/dataprotection)

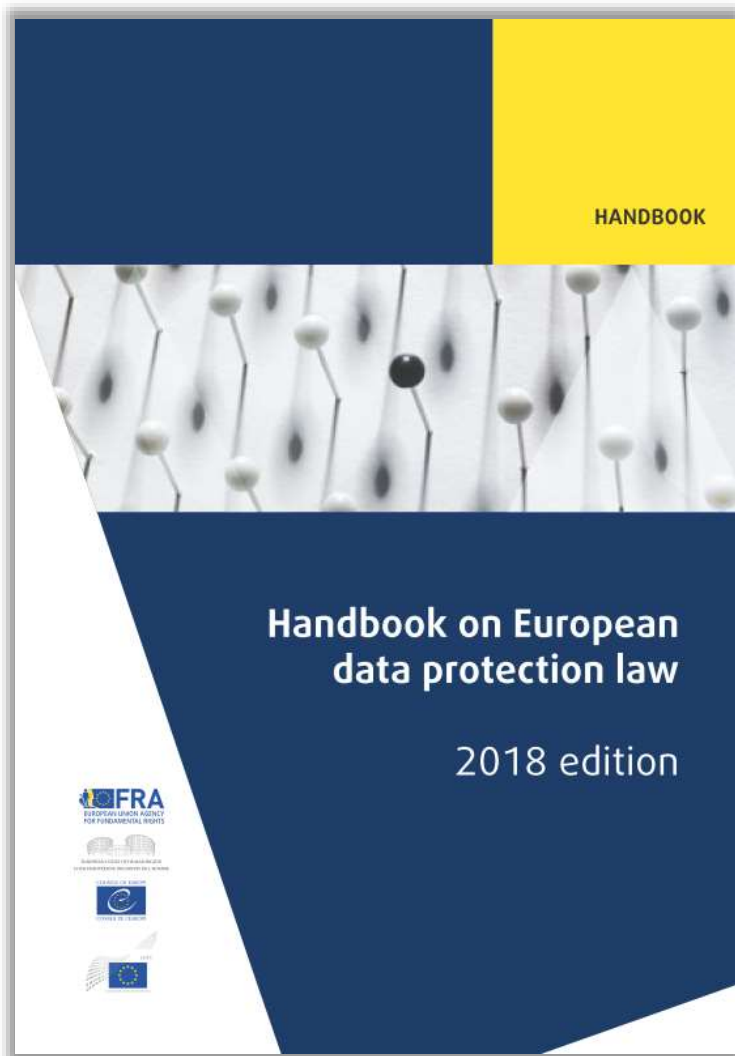
Search tool

ECHR Factsheets

- † Personal data protection
- † New technologies

Contact us

## 612 Руководство по законодательству о защите данных от FRA



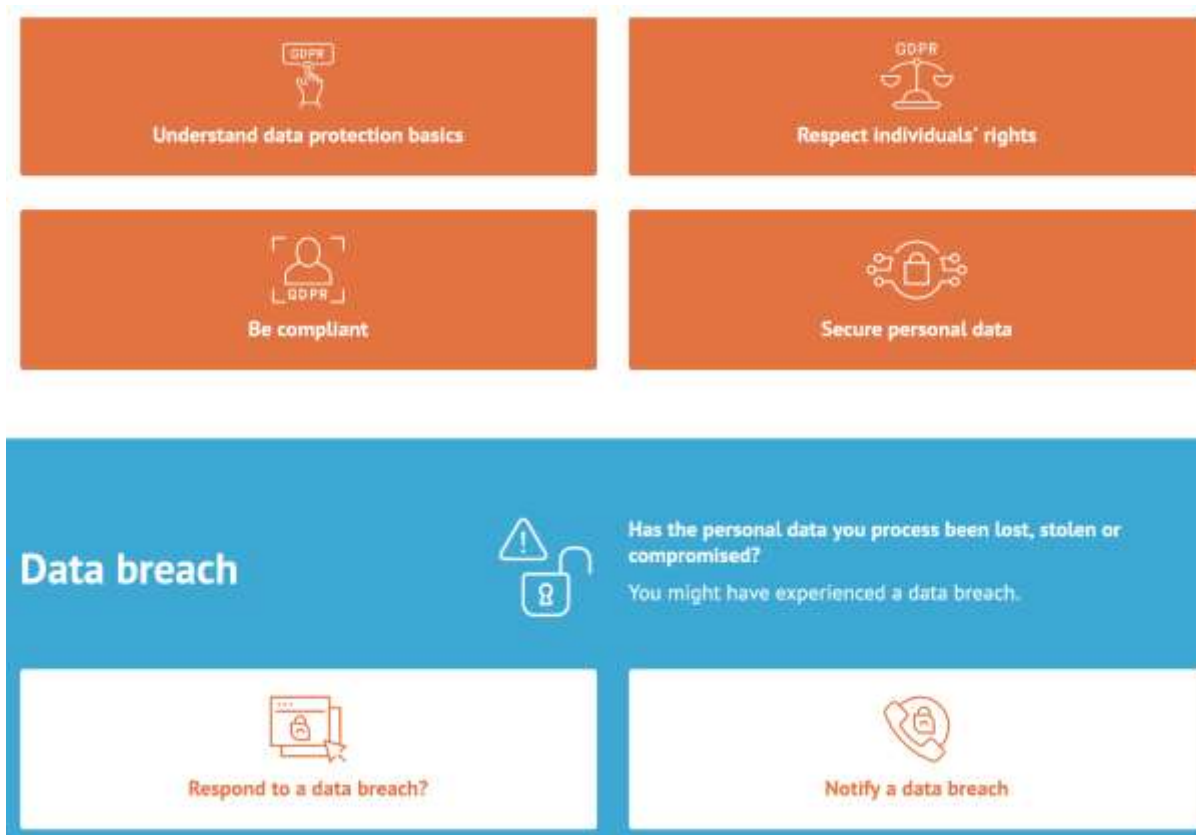
В мае 2018 года Агентство Европейского союза по фундаментальным правам человека (European Union Agency for Fundamental Rights) и Совет Европы (Council of Europe) опубликовали обновленное **Руководство по европейскому законодательству о защите данных**. Положения Руководства охватывают не только основные определения, принципы и требования GDPR, но и рассматривают применимую судебную практику Европейского суда по правам человека (European Court of Human Rights) и Европейского суда (European Court of Justice).



## 613 Руководство EDPB по GDPR для малого бизнеса

Европейский совет по защите данных (EDPB) 27.04.2023 запустил онлайн-руководство для малого и среднего бизнеса по соблюдению GDPR. В руководстве рассматриваются следующие вопросы:

- ◇ основы защиты данных, такие как сфера применения GDPR и определение персональных данных;
- ◇ права субъектов данных;
- ◇ защита данных по проекту и по умолчанию (PBDD);
- ◇ записи о деятельности по обработке данных (RoPA);
- ◇ оценки воздействия на защиту данных (DPIA);
- ◇ уведомления о нарушении безопасности данных (DBN).



## 614 Руководство итальянского Garante по соблюдению GDPR



01.06.2023 итальянский орган по защите данных (Garante) опубликовал новую редакцию руководства по применению GDPR. Руководство адресовано организациям как государственного, так и частного сектора, и особенно малым и средним предприятиям. В нем предлагается обзор основных аспектов, которые компании и государственные учреждения должны иметь в виду для полного соблюдения GDPR (например, права субъектов данных, обязанности контролеров и т.д.).

## 615 Кодекс поведения от ICO по предоставлению данных




Британский надзорный орган ICO (Information Commissioner's Office), в соответствии со ст.121 Data Protection Act 2018, опубликовал для проведения публичных консультаций проект обновленного кодекса поведения по предоставлению данных - Data Sharing Code of Practice - документ, который применяет все правила GDPR для ситуаций, когда компания делится персональными данными с кем-либо еще.

Advice and guidance for all small organisations, including small- to medium-sized enterprises (SMEs), small businesses, sole traders, small charities, groups and clubs, and small start-ups.

Register now →

What's new? →






Get support →



**Five simple ways to make a data protection complaint easier to handle**  
Simple tips on how to handle data protection complaints











### Start here

A quick run-through of the data protection basics for small organisations, including small businesses and sole traders

-  **Find the right resource**  
A handy library of resources you'll find on the data protection advice hub for small organisations.
-  **The benefits of data protection laws**  
A brief introduction to data protection and why it matters for your business, company or group.
-  **Getting started with data protection - top tips for beginners**  
Not sure where to start? Top tips for protecting your data and taking your first steps towards compliance.
-  **Data protection fee: what you need to do**  
Find out if you need to pay. Most small companies only need to pay £40 a year, and some are exempt.
-  **Key data protection terms you need to know**  
Make sense of data protection with our short guide to the key terms you'll need to get started

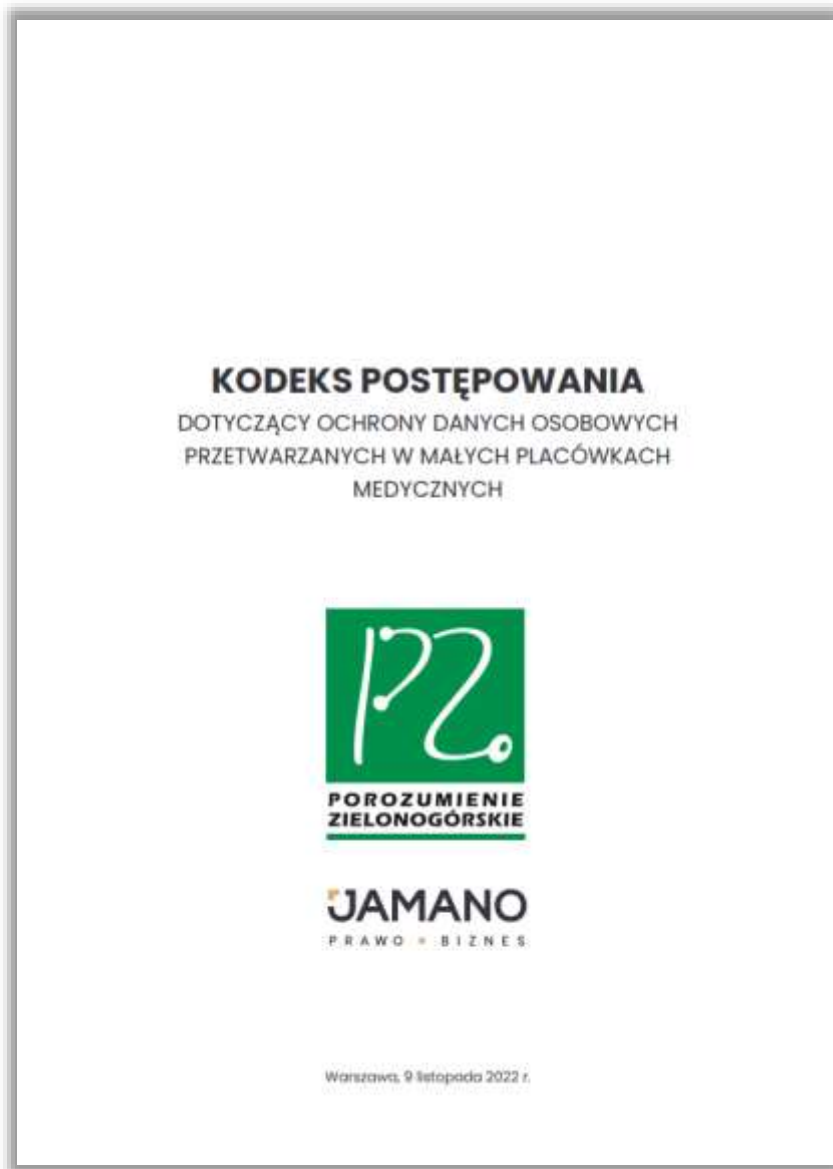
### Check how you're doing

Reliable, bite-sized advice on how to build trust and save money through stronger data protection compliance

-  **Make your own privacy notice**
-  **How to deal with a request for information: a step-by-step guide**
-  **How compliant are you? Check now**
-  **[72 hours - how to respond to a personal data breach](#)**
-  **Understanding and assessing risk in personal data breaches**
-  **How to minimise the risk of personal data breaches happening**
-  **Common data protection mistakes (and how to fix them)**
-  **Four simple ways to make your next subject access request easier to handle**
-  **How to deal with data protection complaints you receive as a small business**
-  **Frequently asked questions**



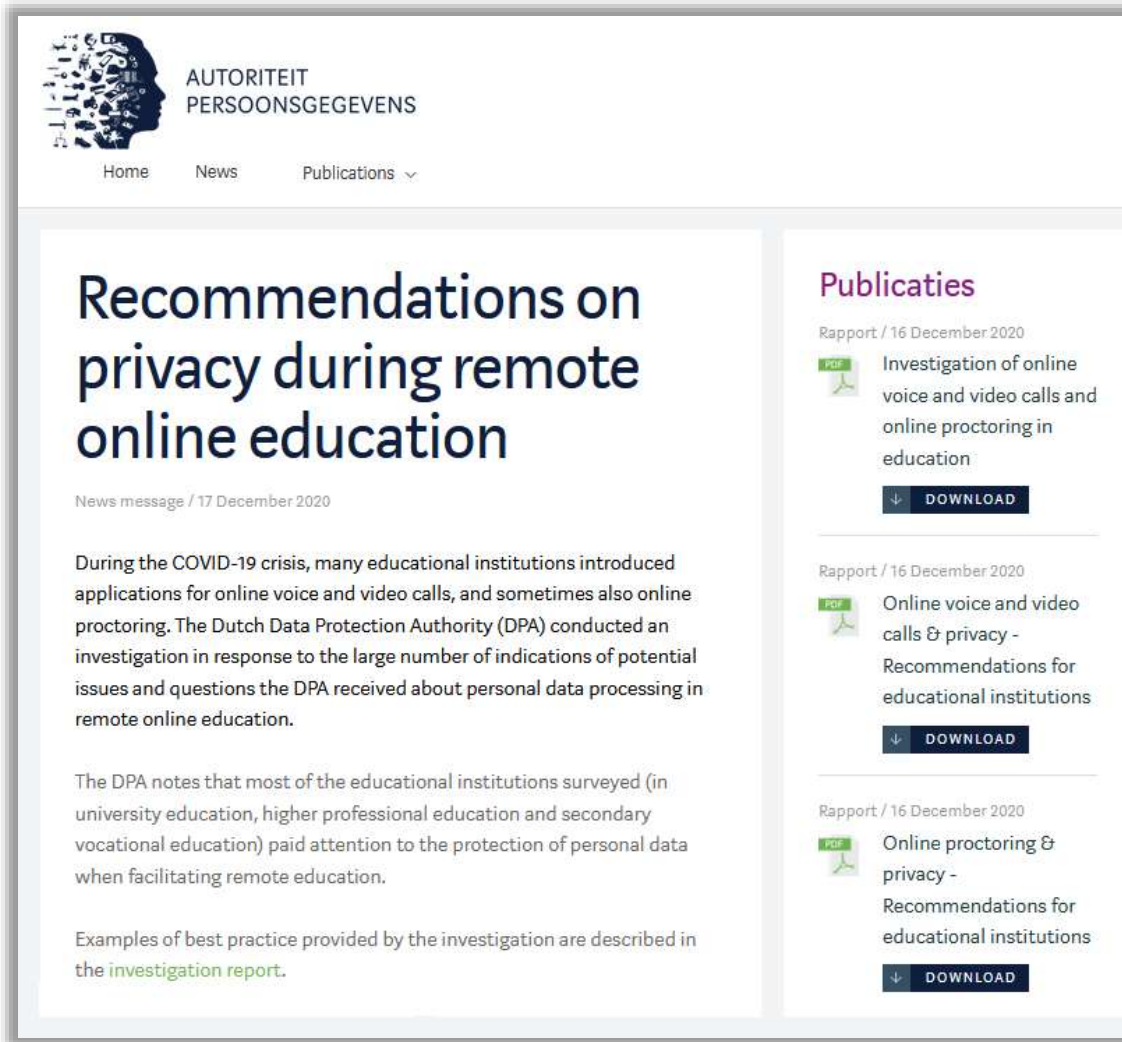
## Кодекс поведения от польского UODO по защите персональных данных в небольших медицинских учреждениях



Польский орган по защите данных ("UODO") 14.12.2022 года объявил, что он утвердил "Кодекс поведения по защите персональных данных, обрабатываемых в небольших медицинских учреждениях", разработанный Федерацией ассоциаций работодателей здравоохранения. Представленный Федерацией кодекс поведения соответствует положениям GDPR и является адекватной гарантией в области защиты данных, предусмотренной его положениями.

Задачей кодекса поведения является обеспечение защиты персональных данных пациентов и других лиц в медицинских учреждениях, помощь медицинским организациям в выполнении требований GDPR и распространение знаний о защите данных среди пациентов. UODO уточнило, что аккредитовало компанию RS Jamano SP. z o.o. sp.k., которая будет выступать в качестве контролера применения кодекса.

## Исследование и рекомендации от АР по дистанционному образованию и онлайн-прокторинга



**AUTORITEIT PERSOONSGEGEVENS**

Home News Publications ▾

# Recommendations on privacy during remote online education

News message / 17 December 2020


During the COVID-19 crisis, many educational institutions introduced applications for online voice and video calls, and sometimes also online proctoring. The Dutch Data Protection Authority (DPA) conducted an investigation in response to the large number of indications of potential issues and questions the DPA received about personal data processing in remote online education.

The DPA notes that most of the educational institutions surveyed (in university education, higher professional education and secondary vocational education) paid attention to the protection of personal data when facilitating remote education.

Examples of best practice provided by the investigation are described in the [investigation report](#).


### Publicaties

Rapport / 16 December 2020

 Investigation of online voice and video calls and online proctoring in education


[DOWNLOAD](#)

Rapport / 16 December 2020

 Online voice and video calls & privacy - Recommendations for educational institutions

[DOWNLOAD](#)

Rapport / 16 December 2020

 Online proctoring & privacy - Recommendations for educational institutions

[DOWNLOAD](#)

### Checklist for online voice and video calls

Getting started	
<input type="checkbox"/>	determine purpose and legal basis
<input type="checkbox"/>	determine necessity
<input type="checkbox"/>	perform a DPIA
<input type="checkbox"/>	seek cooperation with others
Procurement	
<input type="checkbox"/>	select a supplier
<input type="checkbox"/>	draft a data processing agreement
Preparation and instructions	
<input type="checkbox"/>	draft policies
<input type="checkbox"/>	provide information and instruction
<input type="checkbox"/>	rights of students, pupils and parents
<input type="checkbox"/>	be prepared for incidents

### Checklist for proctoring

Getting started	
<input type="checkbox"/>	determine the purpose
<input type="checkbox"/>	determine the necessity
<input type="checkbox"/>	limit infringements of privacy
<input type="checkbox"/>	determine the legal basis
<input type="checkbox"/>	perform a DPIA
<input type="checkbox"/>	seek cooperation with others
Procurement	
<input type="checkbox"/>	select a supplier
<input type="checkbox"/>	draft a data processing agreement
Preparation and instructions	
<input type="checkbox"/>	draft policies
<input type="checkbox"/>	provide information and instruction
<input type="checkbox"/>	rights of pupils/students
<input type="checkbox"/>	be prepared for incidents

## Рекомендации французского CNIL по удаленному мониторингу онлайн-экзаменов (онлайн-прокторингу)

Французский орган по защите информации (CNIL) опубликовал 04.09.2023 рекомендации, касающиеся условий применения устройств удаленного мониторинга для проведения онлайн-экзаменов. Данная рекомендация служит руководством для установления справедливого баланса между борьбой с мошенничеством при сдаче дистанционных экзаменов и защитой прав и свобод граждан.

В рекомендациях указывается на необходимость учитывать принципы защиты данных и права субъектов данных, предусмотренные GDPR. Образовательные учреждения также должны обратиться к своему DPO, чтобы убедиться, что системы удаленного мониторинга любого рода соответствуют нормативным требованиям по защите данных.

Учебным заведениям рекомендуется заблаговременно сообщать о предусмотренных методах проведения экзаменов, а также об устройствах, которые будут использоваться для дистанционного мониторинга, чтобы учащиеся могли сделать свой выбор в пользу того или иного обучения с полной информированностью. Кроме того, следует как можно раньше и точнее информировать студентов об организационных и технических условиях сдачи экзаменов, учитывая сложности дистанционной сдачи, и как можно чаще предоставлять возможность очной сдачи экзамена.

Использование дистанционной оценки, требующей осуществления дистанционного контроля, не должно являться удобной альтернативой, предназначенной исключительно для того, чтобы сделать оценку менее строгой или дорогостоящей. Сдача экзамена в помещении под наблюдением человека по-прежнему рассматривается рекомендацией как наиболее приемлемый способ гарантировать отсутствие мошенничества. Соответственно, очные экзамены должны систематически предлагаться кандидатам, а использование дистанционного контроля не должно быть более эффективным, чем очный контроль.

Что касается технологий, на которые распространяется действие рекомендации, то на cookie-файлы и другие устройства слежения, применяемые в недоступных для общественности сетях, таких как интрасети или экстрасети на основе виртуальной частной сети (VPN), требования рекомендации не распространяются.

Контролеры данных должны проводить оценку воздействия на защиту данных (DPIA) в тех случаях, когда устройства удаленного мониторинга представляют высокий риск для прав и свобод учащихся, а перед экзаменом должно быть проведено тестирование устройств на репрезентативной панели оборудования, которое будет использоваться. В тех случаях, когда не удается найти справедливый баланс между эффективностью дистанционного мониторинга и интрузивностью используемого устройства, следует рассмотреть возможность проведения очного экзамена. При этом соразмерность устройств дистанционного мониторинга должна учитывать контекст и задачи экспертизы.

Устройства удаленного мониторинга, осуществляющие автоматический анализ, являются особенно интрузивными, а проверка кандидатов с помощью обработки биометрических данных может быть уместна в тех случаях, когда число студентов особенно велико.

Кандидаты должны быть проинформированы о том, что подключение к онлайн-экзаменационной платформе требует определенных форм дистанционного мониторинга, однако используемые методы дистанционного мониторинга и характер собираемых данных должны быть указаны до подключения к платформе.

# Руководство CNIL по логированию и журналированию действий субъектов и действий по обработке данных

**CNIL**  
COMMISSION NATIONALE  
INFORMATIQUE ET LIBERTÉS

**Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation**

Lien Légifrance : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044272396>

La Commission nationale de l'informatique et des libertés ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD) ;

Vu la directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision cadre 2008/977/JAI du Conseil ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8-I-2°-b), ci-après loi « informatique et libertés » ;

Après avoir entendu le rapport de M. François PELLEGRINI, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement ;

**Adopte la présente recommandation :**

1. La présente délibération constitue une recommandation relative aux modalités de conservation et d'usage des données de journalisation. Elle vise à faciliter la mise en conformité des différents responsables de traitement, et tient compte d'échanges avec des parties prenantes et du résultat de la consultation organisée sur ce sujet. Cette recommandation, et notamment les exemples qui y sont proposés, n'est ni prescriptive ni exhaustive et a pour seul objectif d'aider les professionnels concernés dans leur démarche de mise en conformité.
2. Les dispositifs de journalisation sont définis comme des dispositifs qui permettent d'assurer une traçabilité des accès et des actions des différents utilisateurs habilités à accéder aux systèmes d'information (et donc aux traitements de données à caractère personnel qui sont susceptibles de constituer ces systèmes). Ces dispositifs peuvent être adossés soit à des applications (qui sont les briques logicielles spécifiques au traitement mis en œuvre et sont donc sujettes à la mise en œuvre de journaux dits « applicatifs »), soit à des équipements spécifiques (qui sont des équipements informatiques associés à des logiciels embarqués, sujets à la mise en œuvre de journaux dits « périmétriques »). La présente recommandation est applicable aux dispositifs de journalisation liés à l'application sur laquelle repose le traitement et non à la journalisation périmétrique, qui répond à une logique différente.

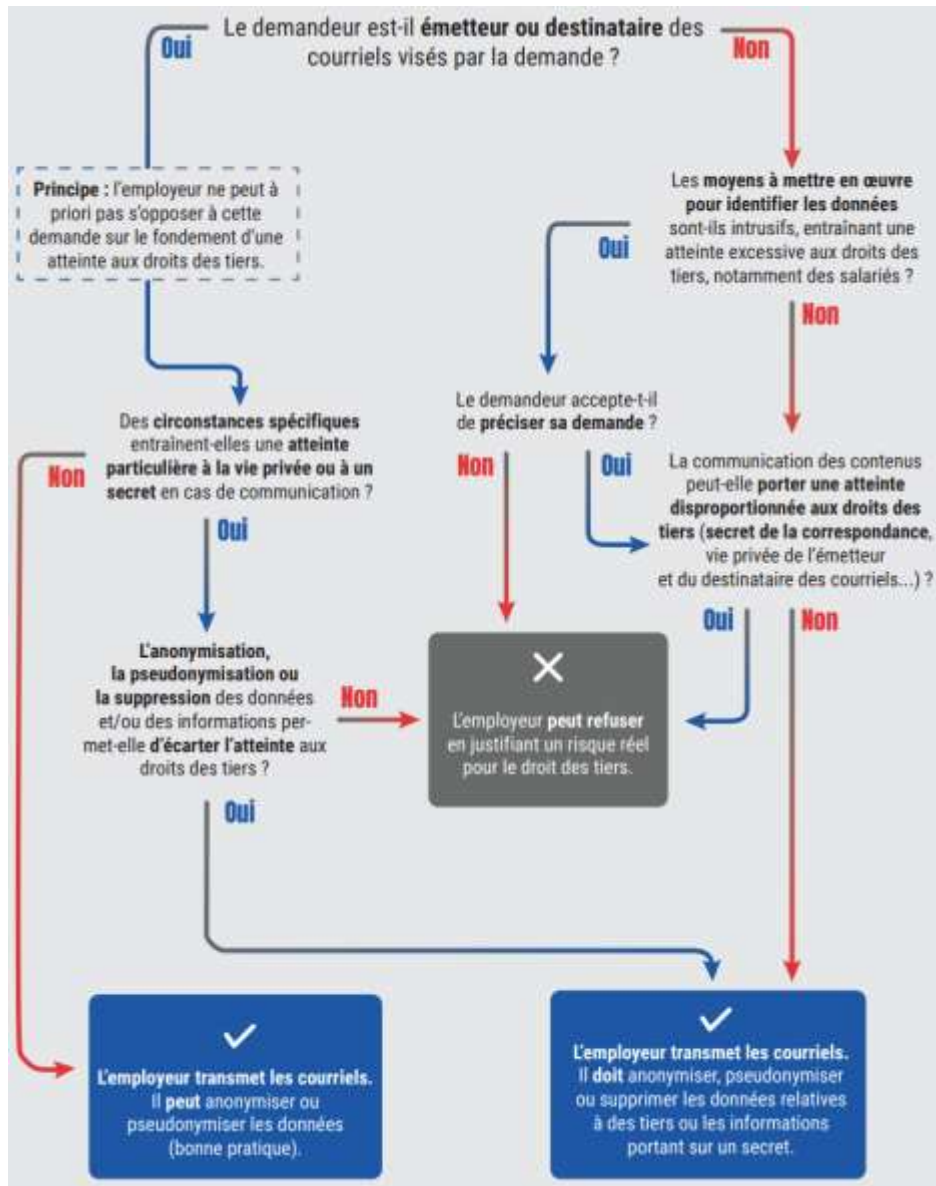
RÉPUBLIQUE FRANÇAISE

3 Place de Fontenay, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - [www.cnil.fr](http://www.cnil.fr)

Les données personnelles relatives à l'exercice des missions de la CNIL sont traitées dans des fichiers distincts à son usage strict. Les personnes concernées peuvent exercer leurs droits d'informatique et libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : [www.cnil.fr/donnees-personnelles](http://www.cnil.fr/donnees-personnelles).

	Durée minimale	Durée maximale	Conditions
Journalisation "standard"	Six mois	Un an	
Journalisation de traitements comportant des données dont la durée de conservation est inférieure à six mois	Six mois	Un an	Les journaux doivent ne pas inclure de données personnelles du traitement principal
Journalisation de traitements faisant l'objet de mesure de "contrôle interne"	Six mois	Trois ans dans les cas les plus courants	Démontrer le risque de détournement pour les personnes concernées par le traitement et disposer de procédures d'analyses et d'investigation documentées
Journalisation de traitements présentant des spécificités particulières	Six mois	A définir dans le cas d'une analyse au cas par cas	Existence d'une spécificité qui peut par exemple être une obligation légale de conservation, une finalité spécifique ou un état de la menace justifiant un allongement

## Руководство CNIL о праве работников на доступ к своим данным и служебной электронной почте



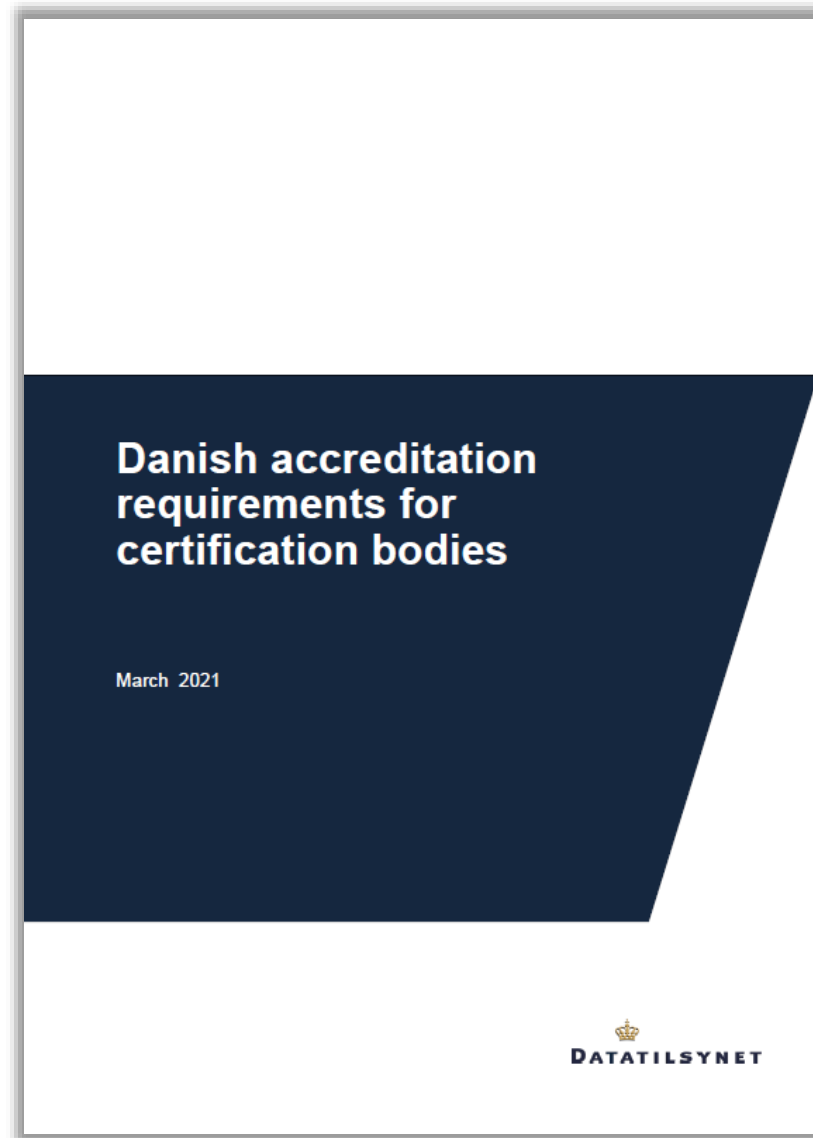
Французский надзорный орган по защите данных (CNIL) 05.01.2022 опубликовал руководство о праве работников на доступ к своим данным и служебной электронной почте. В руководстве изложены правила, касающиеся права доступа, такие как обеспечение проверки личности, обеспечение бесплатного ответа на запрос и обеспечение того, чтобы право доступа не нарушало права третьих лиц.

Руководство описывает как работодатели должны реагировать на работника, который хочет получить доступ или получить копию переписки из служебной электронной почты, отмечая, что работодатель должен оценить возможное нарушение прав третьих лиц, чьи данные могут содержаться в такой переписке.

## Руководство датского Datatilsynet по аккредитации для сертифицирующих органов согласно ст.43 GDPR



The screenshot shows the top part of a news article on the Datatilsynet website. At the top left is the Datatilsynet logo, which includes a crown icon and the text 'DATATILSYNET'. To the right of the logo are two menu items: 'DATABESKYTTELSE' and 'EMNER'. Below the logo is a breadcrumb trail: 'Du er her: Forside / Presse og nyheder / Nyhedsarkiv / 2021 / mar / Supplerende akkrediteringskrav for certificeringsorganer'. The main title of the article is 'Supplerende akkrediteringskrav for certificeringsorganer'. Below the title, it says 'Publiceret 30-03-2021' and 'Nyhed'. The first paragraph of the article reads: 'For at blive et akkrediteret certificeringsorgan skal man bl.a. opfylde en række krav, som er udarbejdet af Datatilsynet. Datatilsynet offentliggør nu disse supplerende akkrediteringskrav.' Below the text is a photograph of a wooden stamp resting on a stack of papers on a desk.



The image shows the cover of a document. The top half has a dark blue background with the title 'Danish accreditation requirements for certification bodies' in white text. Below the title, it says 'March 2021'. At the bottom right, there is the Datatilsynet logo, which consists of a crown icon and the text 'DATATILSYNET'.

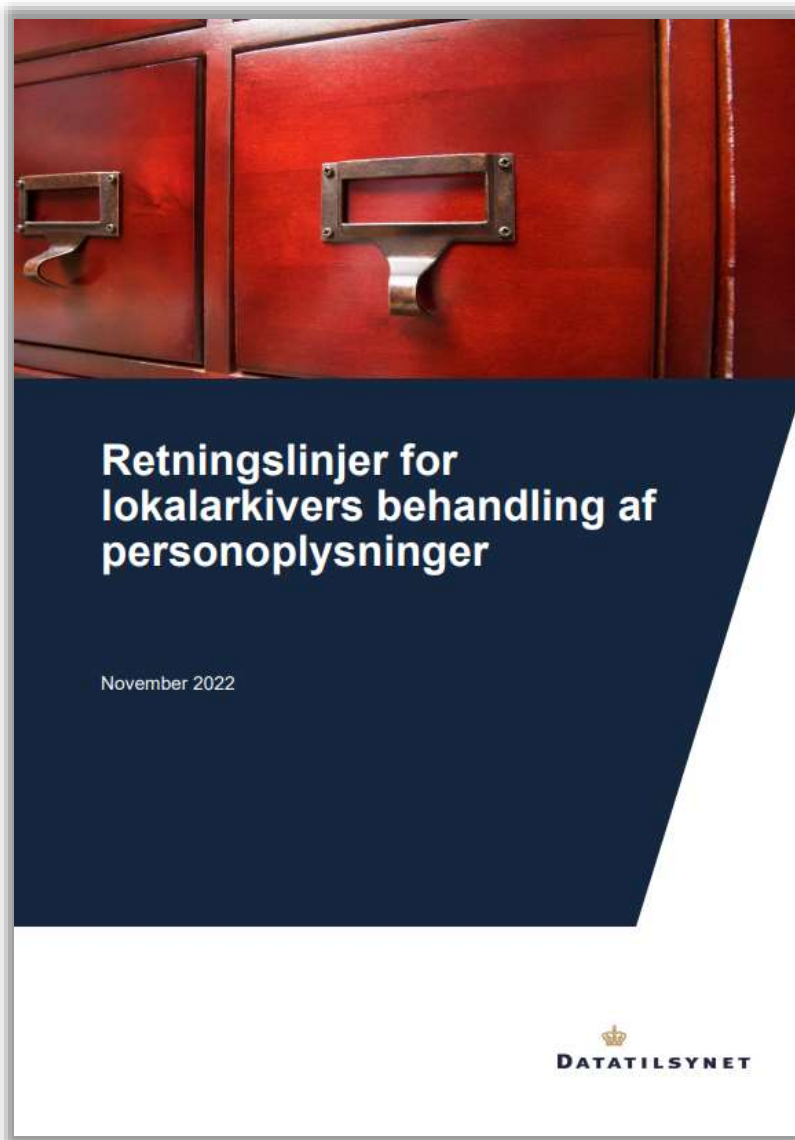
## Руководство по защите данных для архивных служб от EAG



Европейская группа по архивам (EAG - European Archives Group) опубликовала **Руководство по применению GDPR и защите персональных данных для архивных служб**. Это руководство содержит базовые сведения и практические рекомендации для архивистов по конкретным проблемным вопросам, связанных с применением GDPR в архивной сфере.

Руководство адресовано государственным и частным органам и учреждениям, в которых хранятся архивные документы (то есть те документы, которые были отобраны на постоянное хранение), включая национальные и государственные, региональные и муниципальные архивы, музеи, библиотеки, фонды и другие государственные и частные организации, сохраняющие архивные документы.

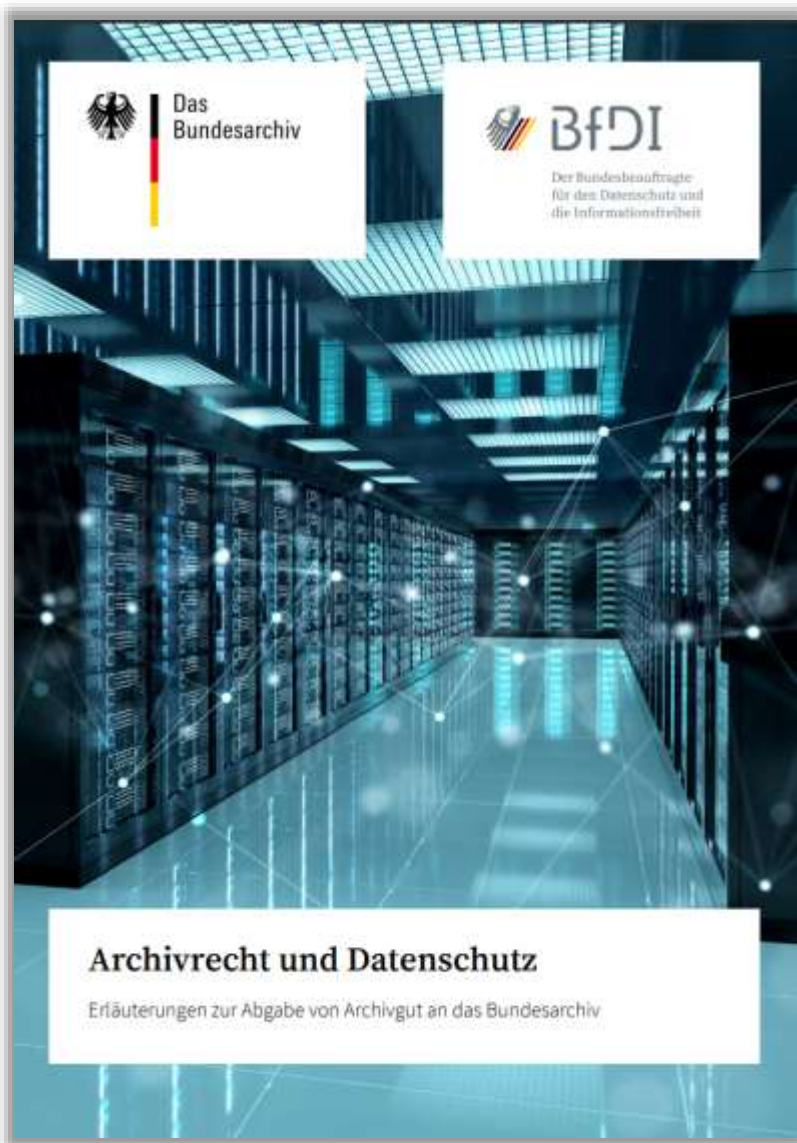
## 624 Руководство по защите данных для архивных служб от датского Datatilsynet



Датский орган по защите данных ("Datatilsynet") 07.11.2022 объявил о публикации руководства по обработке персональных данных местными архивами, чтобы правила защиты данных не препятствовали работе местных архивов. Datatilsynet заявил, что предварительно встречался с представителями местных архивов, чтобы получить представление о проблемах защиты данных, с которыми они сталкиваются ежедневно, и в конечном итоге способствовать тому, чтобы руководство было максимально понятным и практичным. Руководство содержит четыре конкретных указания, которым Datatilsynet рекомендует следовать местным архивам.



## 625 Брошюра немецкого VfDI о архивном праве и защите данных



Федеральный уполномоченный по защите данных и свободе информации ("VfDI") опубликовал 29.03.2023 брошюры под названием "Архивное право и защита данных" в сотрудничестве с Федеральным архивом ФРГ. В брошюре содержатся ответы и общая информация по темам архивного дела и защиты данных, особенно для ответственных за защиту данных ("DPO") и сотрудников, работающих в управлении делами федеральных органов власти.

Брошюра дает представление о таких вопросах, как архивирование и обработка персональных данных в целях, представляющих общественный интерес; применение GDPR к архивам; защита прав и свобод субъектов данных в контексте архивов; технические и организационные меры, принятые Федеральным архивом.

[https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2023/06\\_Broschuere-Archivrecht.html](https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2023/06_Broschuere-Archivrecht.html)

[https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/Archivrecht.pdf?\\_\\_blob=publicationFile&v=3](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/Archivrecht.pdf?__blob=publicationFile&v=3)

# Руководство Национального архива Великобритании по архивному хранению персональных данных

## Contents

Foreword.....	4
Summary.....	6
Introduction.....	7
Key concepts.....	8
Scope.....	8
Purpose of this guide.....	9
Responsibilities of the archives sector.....	10
Data protection law and archiving.....	12
Data protection law has changed.....	12
What does the change mean?.....	12
What has changed?.....	13
General Data Protection Regulation (GDPR).....	13
Data Protection Act 2018.....	14
Exemptions.....	14
Safeguards.....	15
What is meant by “substantial damage or distress”?.....	16
Lawful basis for different types of archive service.....	16
Right to Erasure (Right to be forgotten).....	17
Access to data by data subjects.....	18
Unstructured manual records.....	18
Data Protection Officers and records of processing.....	18
Sanctions.....	19
Specific processing.....	19
Dual purpose processing and updating data.....	19
What do I need to do to start?.....	20
Archiving purposes in the public interest.....	21
What is archiving under GDPR.....	21
Establishing ‘archiving purposes’.....	21
Establishing the public interest in archiving.....	22
Criteria for archiving purposes in the public interest.....	24
What archiving in the public interest is not.....	25
Processing for archiving purposes.....	26
Why are there special data protection rules for archiving?.....	26
Appraise (selection).....	27
Acquire.....	28
Security and Preservation.....	29
Arrange and describe – metadata, catalogues and finding aids.....	29
Access.....	31
Communicate / inspect.....	31
Disseminate– publish /online access/exhibition material.....	34
Removing access (takedown and reclosure).....	34
Responsibilities of users of archived personal data.....	35
Annex A Explanation of terms used in this guide.....	36
Annex B Parliamentary Question reply what is meant by the term Archiving in the Public Interest.....	39
Annex C Main references to archiving in GDPR and Data Protection Act 2018.....	41

Activity	Covered by Guide ✓	Not covered by Guide ✗
Business processing before archiving	Bodies holding personal data with the intent that they be part of an archive in the future either as part of their organisation or by transfer to an archives service.	Business purpose storage of data and general information management including offline storage. No intention to preserve beyond business use or records not of enduring value.
Archive service activities	Records received for in-house appraisal as well as material already appraised and held in collections.	Processing by archive services of data not held for archiving in the public interest purposes e.g. for marketing and fundraising or about staff and users.
Archive collections	Public and private bodies and voluntary groups preserving and making personal data directly or indirectly available, either now or in the future, to enable research, provide corporate memory or as continuing evidence of rights and obligations.	Research and re-use by members of the public of records held in or published by archive services.
Other		General compliance with data protection law or for other purposes such as for statistical or scientific and historical research purposes.

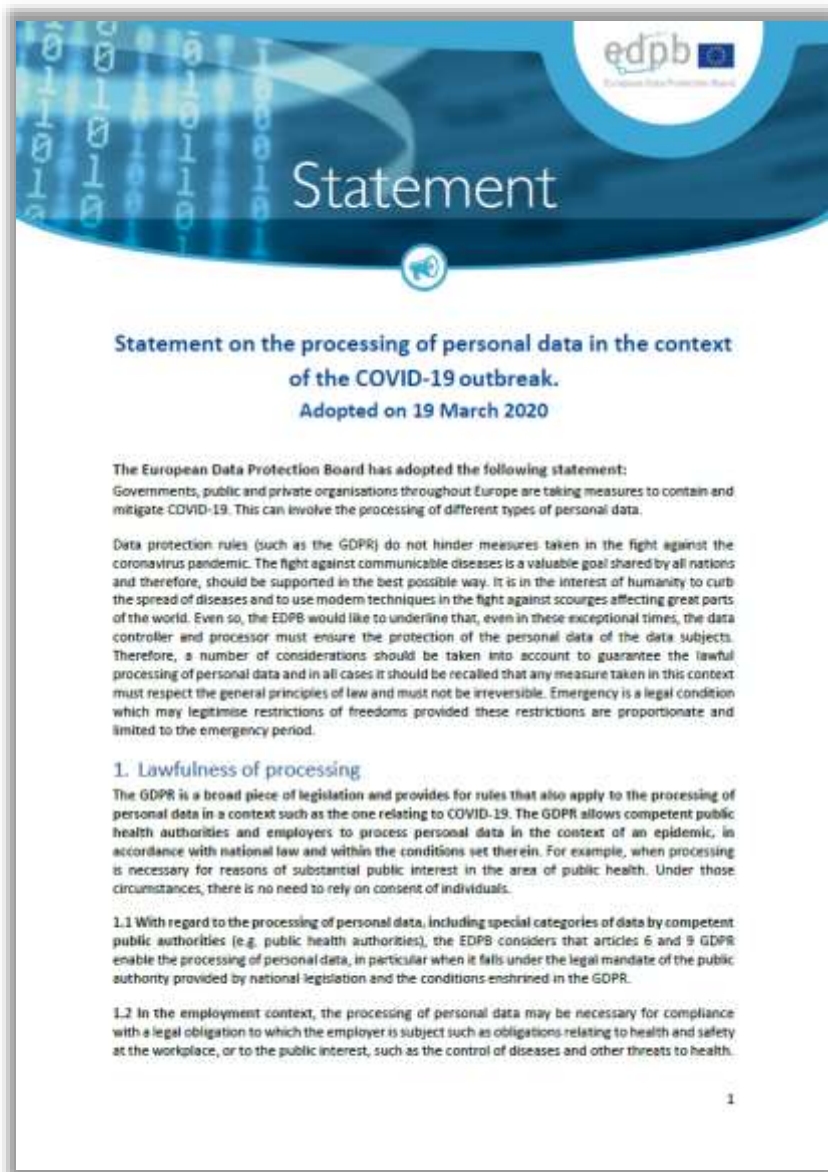
## Правила архивного хранения и удаления данных в соответствии с требованиями защиты данных в государственном секторе Баварии



Баварский орган по защите данных ("BayLfD") 01.012023 выпустил совместный рабочий документ с Главным управлением Баварского государственного архива под названием "Удаление или архивирование? Правила архивного хранения и удаления данных в соответствии с требованиями защиты данных в государственном секторе Баварии". В частности, в рабочем документе подчеркивается взаимосвязь между обязательством по удалению данных в соответствии с законодательством о защите данных и обязательством по предоставлению архивных материалов в соответствии с архивным законодательством.

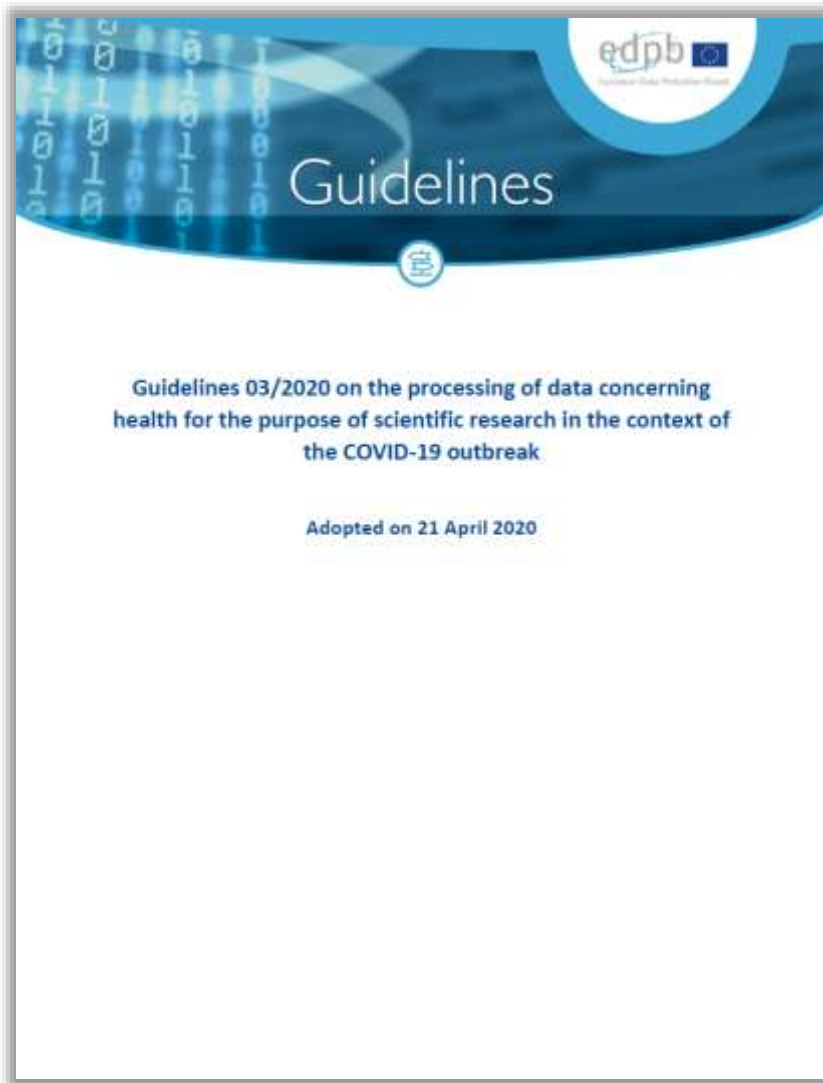
Более подробно в рабочем документе рассматриваются сроки хранения, требования к информации в соответствии с законом о защите данных при архивировании документов, а также проблемы оцифрованного государственного управления. Кроме того, в рабочем документе рассматривается конкретное взаимодействие между законодательством о защите данных и архивным законодательством при преждевременном удалении персональных данных в отдельных случаях.

## Заявление EDPB об обработке персональных данных в контексте пандемии COVID-19

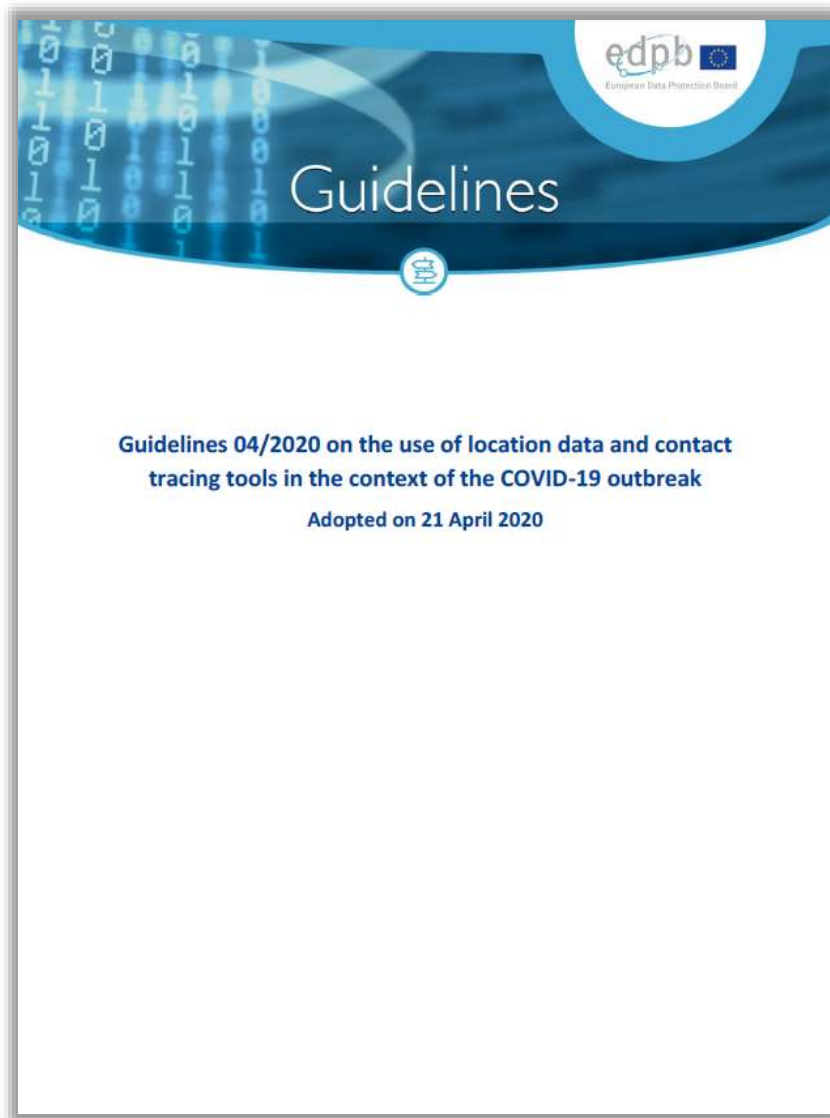


Согласно позиции European Data Protection Board, опубликованной 16.03.2020, действующим законодательством предусмотрены все необходимые правовые основания, позволяющие работодателям и компетентным органам здравоохранения обрабатывать персональные данные в контексте эпидемии COVID-19 без необходимости получения согласий субъектов данных. Это применимо, например, когда обработка персональных данных необходима работодателям по причинам, представляющим общественный интерес в области общественного здравоохранения или для защиты жизненно важных интересов (ст. 6 и 9 GDPR) или для выполнения иных юридически закрепленных обязательств. Также затронут вопрос обработки данных, получаемых с использованием средств электронной связи, таких как данные местоположения из мобильных пользовательских устройств.

## Руководство EDPB по обработке данных о здоровье для научных исследований в контексте вспышки COVID-19



1	Introduction.....
2	Application of the GDPR.....
3	Definitions .....
3.1	“Data concerning health” .....
3.2	“Processing for the purpose of scientific research” .....
3.3	“Further processing” .....
4	Legal basis for the processing.....
4.1	Consent.....
4.2	National legislations .....
5	Data protection principles.....
5.1	Transparency and information to data subjects .....
5.1.1	When must the data subject be informed? .....
5.1.2	Exemptions .....
5.2	Purpose limitation and presumption of compatibility .....
5.3	Data minimisation and storage limitation.....
5.4	Integrity and confidentiality .....
6	Exercise of the rights of data subjects.....
7	International data transfers for scientific research purposes .....
8	Summary .....



Согласно руководству European Data Protection Board, выделяются две основные цели:

1. отслеживание местоположения для моделирования распространения COVID;
2. отслеживание контактов для уведомления о нахождении рядом с подтвержденным носителем COVID.

Для первой цели нужно использовать анонимизированные данные, а использование приложений для отслеживания контактов должно быть добровольным. Кроме того, мобильные приложения по отслеживанию контактов не должны мониторить отдельные действия субъектов.

## Руководство бельгийского L'APD по измерению температуры в контексте вспышки COVID-19

The screenshot shows the website of the Autorité de protection des données (APD) of Belgium. The main navigation bar includes links for 'Plan du site', 'Langue', 'FAQ', 'Presse', 'Liens', and 'Contact'. Below this, there are five main menu items: 'À PROPOS DE L'AUTORITÉ', 'RGPD', 'THÈMES DE VIE PRIVÉE', 'LEGISLATION ET NORMES', and 'DÉCISIONS'. The current page is titled 'Prise de température dans le cadre de la lutte contre le COVID-19'. The main content area contains a paragraph in French stating that the APD notes that in the context of the resumption of social and economic life, data controllers are seeking technological solutions to detect individuals with fever at the entrance of buildings to prevent further contamination. It also mentions that the implementation of such a policy is part of their mission to protect security and health. Below this, there is a section titled 'Une telle prise de température s'effectue au moyen d'un thermomètre classique, de scanners de fièvre digitaux dirigés sur le front de la personne concernée ou de systèmes perfectionnés de caméras thermiques.' followed by a paragraph explaining that while the current situation is challenging, the APD reminds that temperature measurement of physical persons falls under the GDPR if it leads to a personal data processing. A list of obligations for data controllers is provided at the bottom.

Plan du site » Langue » FAQ » Presse » Liens » Contact »

**À PROPOS DE L'AUTORITÉ**  
Pour en savoir plus sur l'Autorité

**RGPD**  
Dossier thématique sur le RGPD

**THÈMES DE VIE PRIVÉE**  
Nos activités quotidiennes

**LEGISLATION ET NORMES**  
Droits de référence relatif à la protection des données

**DÉCISIONS**  
Actes, décisions et recommandations

Accueil » Prise de température dans le cadre de la lutte contre le COVID-19

### Prise de température dans le cadre de la lutte contre le COVID-19

*L'APD constate que dans le cadre de la reprise de la vie sociale et économique, les responsables du traitement cherchent des solutions technologiques en vue de détecter à l'entrée de leurs bâtiments les individus qui présentent de la fièvre afin d'éviter qu'ils n'y pénètrent, et ce dans le but de prévenir d'autres contaminations au sein des bâtiments. Ils considèrent que la mise en place d'une telle politique d'accès fait partie de leur mission (à savoir protéger la sécurité et la santé des personnes concernées).*

Une telle prise de température s'effectue au moyen d'un thermomètre classique, de scanners de fièvre digitaux dirigés sur le front de la personne concernée ou de systèmes perfectionnés de caméras thermiques.

L'APD comprend que la situation actuelle est éprouvante pour chacun mais rappelle que la prise de température de personnes physiques relève du RGPD si cet acte donne lieu en soi ou par la suite à un traitement de données à caractère personnel.

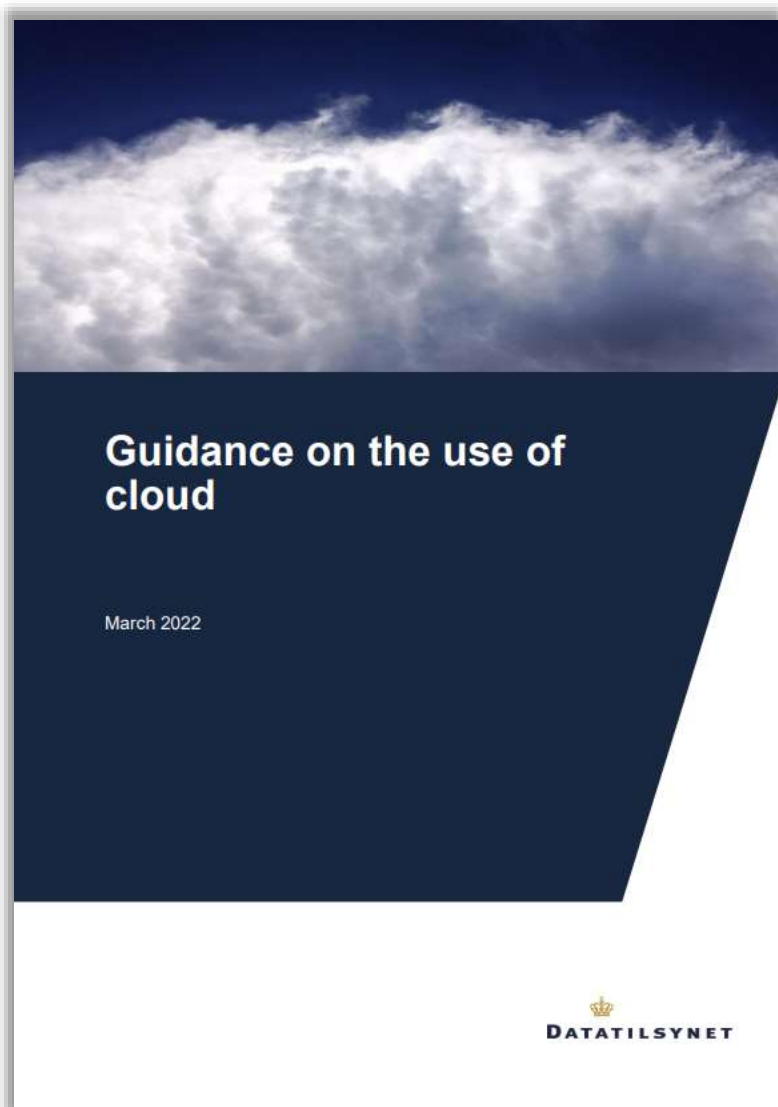
Dans ce cas, les responsables du traitement devront :

- respecter toute une série d'autres obligations en vertu du RGPD comme le fait d'assurer la transparence vis-à-vis des personnes concernées ;
- garantir la sécurité des données ;
- éventuellement réaliser une analyse d'impact relative à la protection des données ; et,
- disposer d'une base légale appropriée pour procéder au traitement.

Бельгийский орган по защите данных, Autorité de protection des données, опубликовал 05.06.2022г. Руководство, согласно которому контролеры данных могут реализовывать политики доступа на объекты недвижимости, которые включают измерение температуры с помощью термометров, цифровых сканеров или тепловизионных камер. В свете этого в Руководстве подчеркивается, что контролеры данных должны, среди прочего, соблюдать GDPR, обеспечивать безопасность данных, осуществлять DPIA при такой необходимости, надлежащим образом выбирать правовое основание для обработки данных.

Кроме того, Руководство предлагает три сценария для оценки применимости GDPR к рассматриваемой активности: обработка сведений о температуре не представляет собой обработку персональных данных, если не фиксируются дополнительные данные или если обработка не осуществляется автоматизировано. Наконец, в Руководстве делается вывод о том, что в отсутствие прямого требований закона контролеры данных могут не проводить индивидуальный температурный контроль с использованием сложных электронных устройств или с целью фиксации результатов такого контроля.

## 632 Руководство датского Datatilsynet по использованию «облачных» сервисов



Датский орган по защите данных (Datatilsynet) опубликовал руководство, предназначенное для контролеров при использовании облачных сервисов, включая краткое описание подводных камней, возможностей и обязательств, возникающих при использовании таких сервисов. Руководство содержит в том числе следующие разделы:

- указания о том, как оценивать обработчиков данных, какие требования к ним следует предъявлять и как обеспечить обработку в соответствии с установленными инструкциями;
- раздел, посвященный передаче данных в третьи страны и, в частности, в США;
- практические вопросы, которые должны задать себе контролеры данных, намеревающиеся использовать облачные сервисы.



## 633 Руководство французского CNIL по обмену персональными данными через API



Французский орган по защите информации (CNIL) 07.07.2023 опубликовал техническую рекомендацию по совместному использованию персональных данных через интерфейс прикладного программирования (API). Под действие рекомендации подпадают все виды обмена персональными данными через API, как открытые, так и ограниченные, и все типы организаций, как государственных, так и частных.

## Заключение нидерландского Autoriteit Persoonsgegevens об обработке данных в контексте научных исследований



Нидерландский орган по защите данных 13.02.2023 опубликовал заключение об исследованиях в области избыточной смертности. AP получил официальный запрос на консультацию от Палаты представителей относительно повторного использования медицинских данных для научных исследований, и пришел к выводу, что предоставление данных о вакцинации исследователям возможно и законно в соответствии с GDPR и правовой базой Статистического управления Нидерландов.

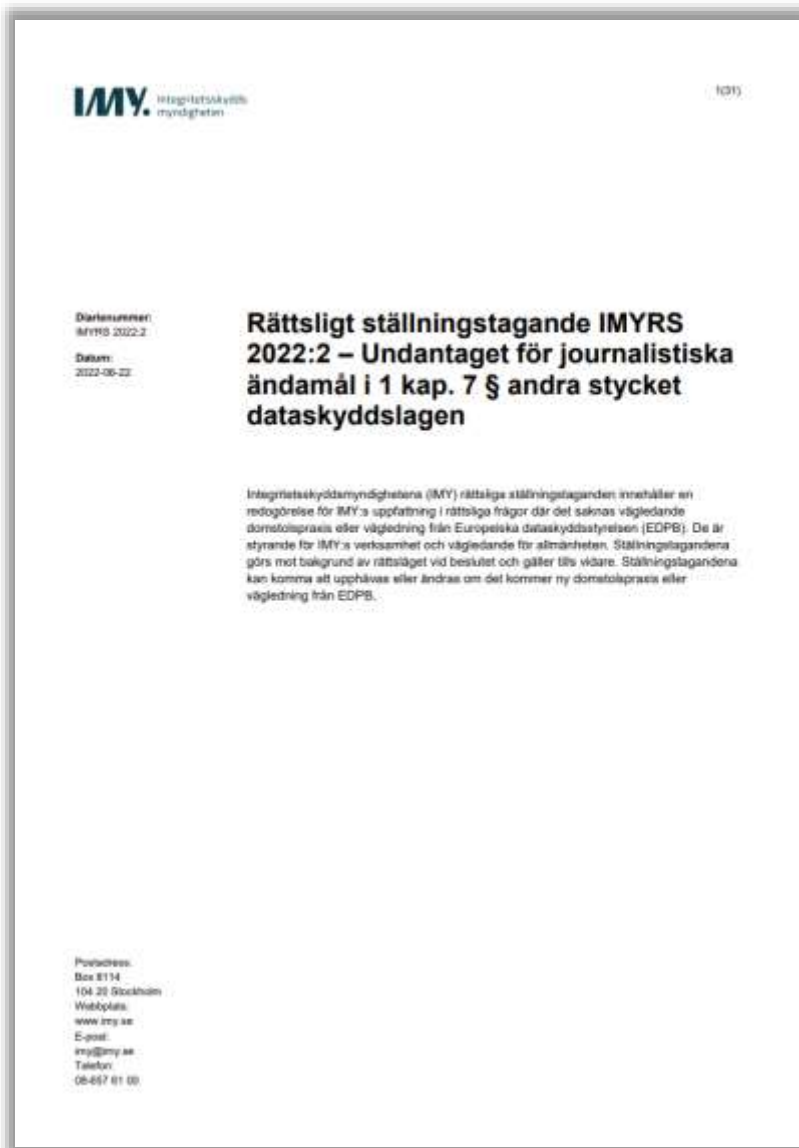
Ст.24 Закона о внедрении GDPR предусматривает толкование исключения из запрета на обработку медицинских данных и предлагает возможность обработки медицинских данных для научных исследований. ЦБС не может запрашивать персональные данные у государственных учреждений на основании ст.33 Закона о Центральном бюро статистики ("Закон о ЦБС") для проведения научных исследований, кроме исследований самого ЦБС. В будущем использование медицинских данных всегда должно быть прозрачным и что все данные, запрашиваемые ЦБС, связаны с проведением статистических исследований ЦБС, а также что данные действительно используются для этой цели. Если ЦБС предоставляет персональные данные исследователям, исследователи должны иметь законное основание в соответствии со ст.6 GDPR и исключение для обработки данных о здоровье в соответствии со ст.9 GDPR.

GDPR не применяется к обработке медицинских данных умерших лиц, но данные, собранные в контексте отношений по лечению, будут оставаться предметом профессиональной тайны и конфиденциальности после смерти.

<https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-onderzoek-naar-oversterfte-kan-cbs>

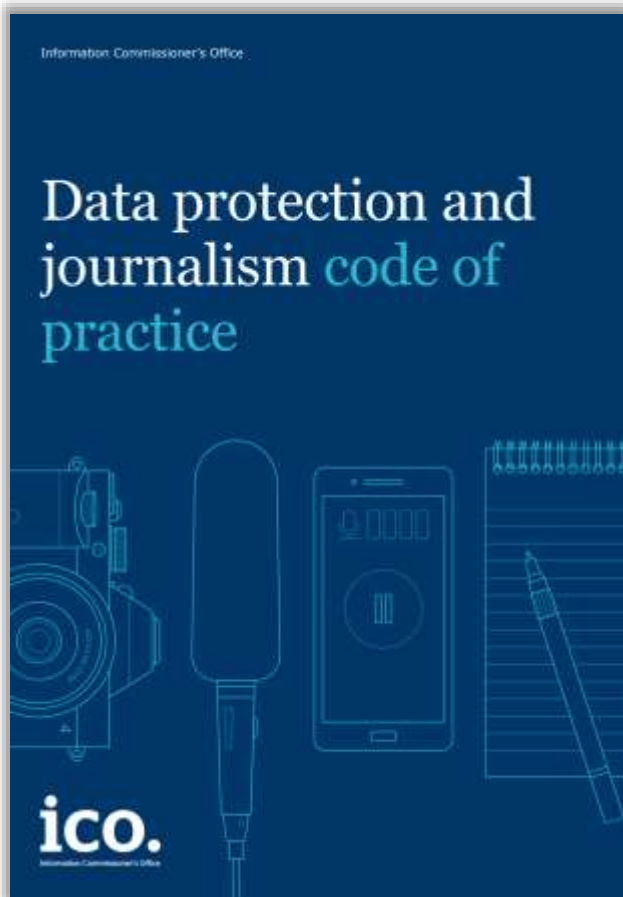
[https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies\\_ap\\_onderzoek\\_oversterfte.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_ap_onderzoek_oversterfte.pdf)

## 635 Заключение шведского IMY об обработке данных для журналистских целей



Шведский орган по защите данных (Integritetsskyddsmyndigheten) 27.06.2022 опубликовал заключение, описывающее ситуации правомерной обработки данных в журналистских и иных связанных целях.

Заключение также содержит десять конкретных примеров различных типов публикаций персональных данных вместе с мнением IMY о том, распространяется ли на них исключение для журналистских целей.



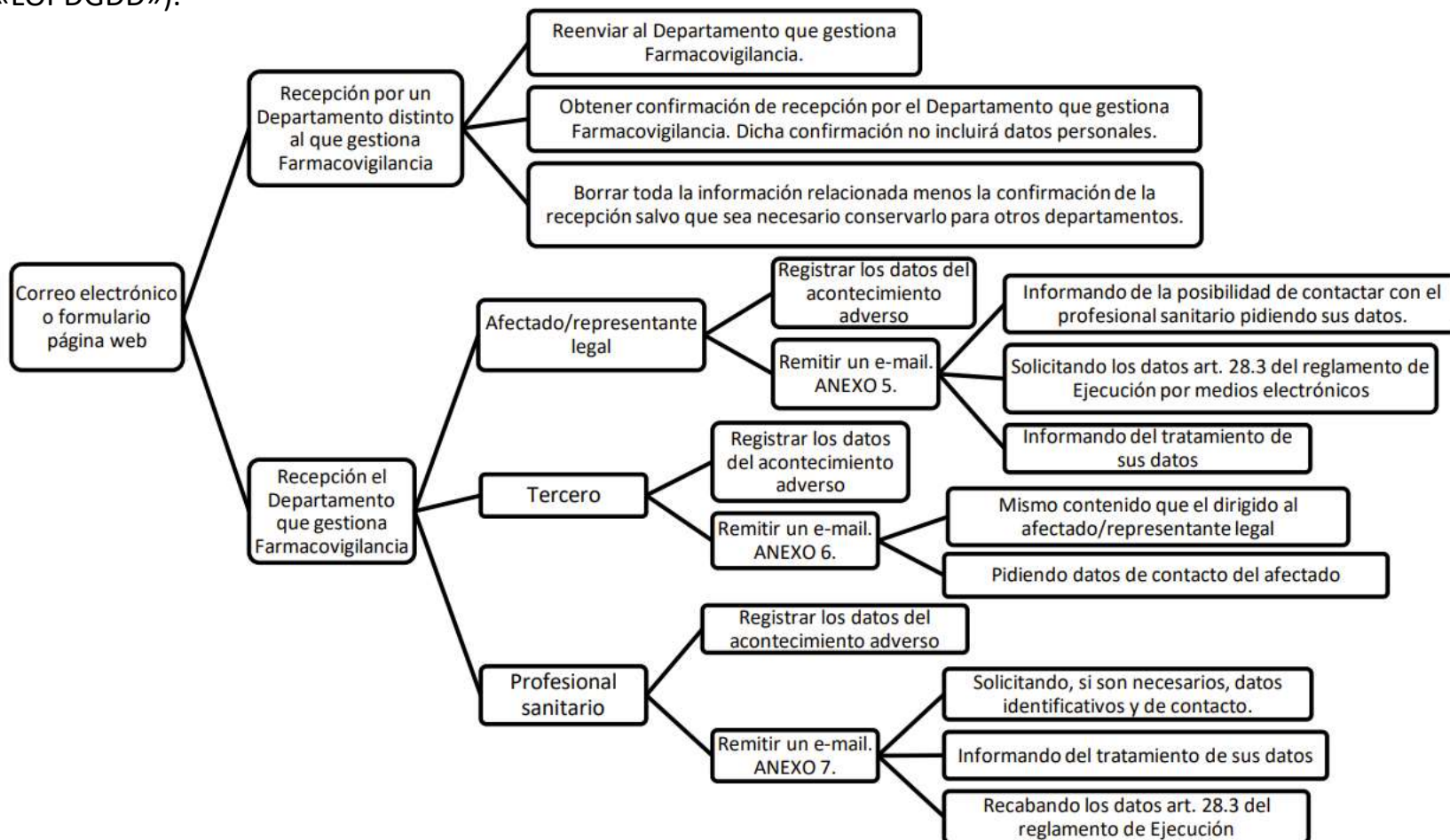
Управление комиссара по информации (ICO) 01.02.2024 года опубликовало Кодекс практики защиты данных и журналистики, который является практическим руководством по соблюдению законов о защите данных и передовой практики при использовании личной информации в журналистских целях.

Любое лицо, использующее персональные данные в журналистских целях, должно в целом соблюдать требования законодательства о защите данных. Кодекс требует, чтобы лица, на которых распространяется его действие могли:

- демонстрировать, как они соблюдают принципы защиты данных;
- обеспечивать безопасность личной информации путем принятия соответствующих и пропорциональных мер безопасности;
- использовать личную информацию на законных основаниях, опираясь на одно из конкретных законных оснований, предусмотренных законодательством о защите данных;
- использовать личную информацию честно и прозрачно;
- использовать только ту личную информацию, которая необходима, и хранить ее только до тех пор, пока она необходима.

## Испанский кодекс о персональных данных в клинических испытаниях, клинических исследованиях и фармаконадзоре

10.02.2022г. испанский орган по защите данных («AEPD») утвердил Кодекс поведения при обработке персональных данных в целях клинических испытаний, других клинических исследований и фармаконадзора, что сделало его первым отраслевым кодексом поведения, который будет утвержден после вступления в силу GDPR. Кодекс был утвержден в соответствии со ст.40 GDPR и ст.38 Органического закона Испании 3/2018 от 05.12.2018г. «О защите персональных данных и гарантиях цифровых прав» («LOPDGDD»).



## Руководство датского Datatilsynet по хранению согласий на обработку данных

Персональные данные, обрабатываемые на основании согласия субъекта данных, включая само согласие, должны, в качестве отправной точки, быть удалены сразу после завершения обработки, см. ст.5(1)(e) и ст.17(1)(b) GDPR. Из последнего положения следует, что субъект данных имеет право на удаление персональных данных, касающихся его или ее, контроллером без неоправданной задержки, и контроллер обязан удалить персональные данные без неоправданной задержки, если субъект данных отзывает согласие, на котором основана обработка, см. ст.6(1)(a) или ст.9(2)(a), и нет другого законного основания для обработки. Однако исключением является, в соответствии со ст.17(3)(e) GDPR, если продолжение обработки персональных данных, включая данное согласие, необходимо для установления, осуществления или защиты юридических претензий.

Необходимость дальнейшей обработки персональных данных подразумевает, что должен существовать законный интерес в сохранении этих данных. Сам по себе факт, что данные могут быть полезны "на всякий случай", не может служить основанием для их дальнейшего хранения.

Поэтому может возникнуть необходимость в качестве контроллера данных сохранить персональные данные для документирования в течение ограниченного периода времени, чтобы выяснить, может ли существовать или возникнуть спор. Продолжительность этого периода должна определяться в каждом конкретном случае, при этом особое значение должно придаваться тому, через какое время после прекращения деятельности по обработке данных может возникнуть спор, в том числе с учетом накопленного опыта.

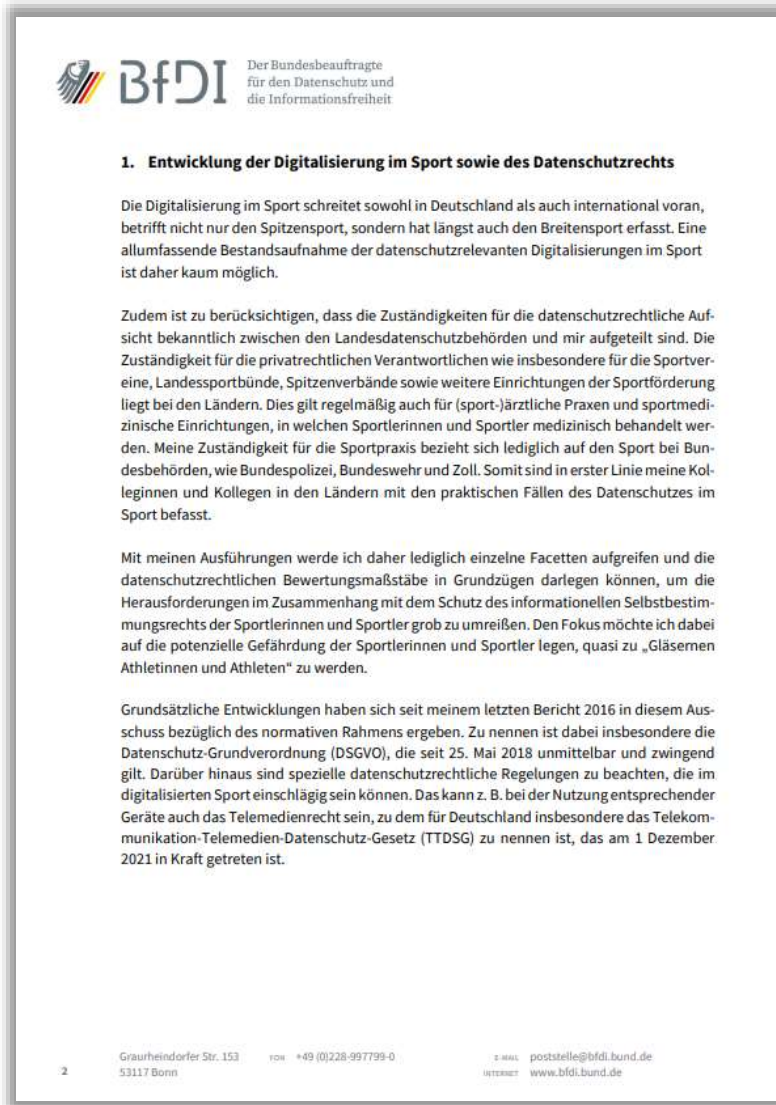
С другой стороны, сохранение данных не будет соответствовать требованию необходимости, если существует лишь гипотетический интерес в сохранении персональных данных. Например, если личные данные сохраняются исключительно - и без учета конкретных обстоятельств - потому что в будущем может быть подана жалоба или что-то подобное. Таким образом, общие сроки давности сами по себе не могут служить основанием для отказа от удаления персональных данных.

В качестве иллюстрации вышесказанного можно привести случай обработки персональных данных компанией SmartResponse, когда Датское агентство по защите данных установило, что срок хранения в 5 лет, определенный на основании срока давности в разделе 41(7) Закона о защите данных, не соответствует требованию необходимости в ст.5(1)(e) GDPR, поскольку простая возможность того, что в будущем может быть возбуждено уголовное дело, не оправдывает и не требует хранения персональных данных в течение 5 лет.



◇ Греческий орган по защите данных ("HDPA") опубликовал 31.03.2023 руководство по политической коммуникации для органов и лиц, осуществляющих политическую коммуникацию и являющихся контролерами данных в соответствии с GDPR. Руководство разъясняет, что если член парламента или кандидат в депутаты получает данные от своей политической партии и обрабатывает эти данные для своей личной политической коммуникации, то в таких обстоятельствах он становится контролером.

◇ Руководство разъясняет, что в тех случаях, когда обработка данных поручается процессорам, например, компаниям, рассылающим письма, SMS или электронные сообщения, процессор должен следовать применимым обязанностям, подробно описанным в GDPR. В руководстве оговаривается, что оно не распространяется на коммуникации, осуществляемые другими общественными или профессиональными организациями, такими как палаты, профессиональные ассоциации и профсоюзы.



◇ Федеральный уполномоченный по защите данных и свободе информации в ФРГ ("BfDI") опубликовал 27.03.2023 свое мнение о защите данных в спорте, в котором излагаются общие принципы и требования законодательства о защите данных, а также конкретные аспекты цифровизации в спорте, чтобы подчеркнуть проблемы, связанные с защитой права спортсменов на информационную приватность.

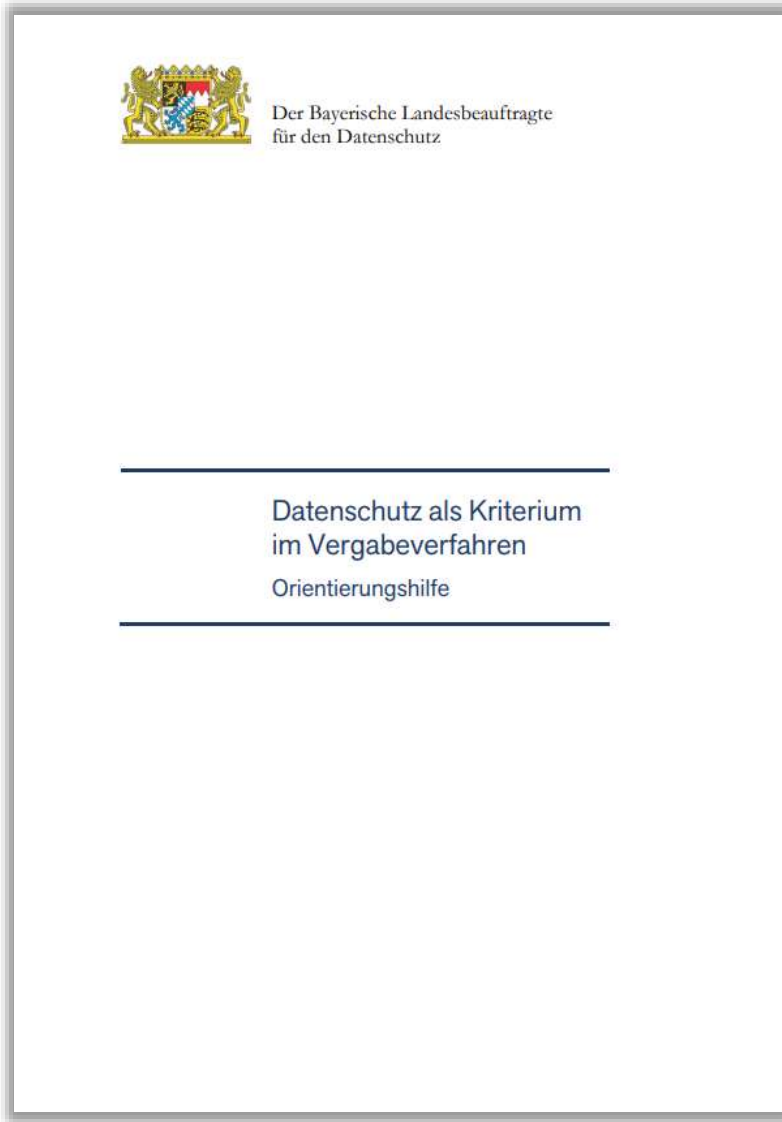
◇ Так, в отношении обработки данных спортсменов применяется не только GDPR, но и специальные положения о защите данных, которые могут быть актуальны в условиях цифровизации спорта, например, Федеральный закон о регулировании защиты данных и конфиденциальности в сфере телекоммуникаций и телемедиа от 23.06.2021 ("TTDSG").

◇ В соревновательном спорте обрабатывается большое количество персональных данных спортсменов для измерения и оптимизации спортивных результатов, при этом некоторые из этих персональных данных, например, касающиеся травм или показателей крови, представляют собой специальные персональные данные в значении ст.9(1) GDPR - как данные о здоровье.

◇ Также отмечается, что соревновательный спорт часто предполагает трудовые отношения и, соответственно, данные спортсменов обрабатываются работодателем в целях трудовых отношений, что влечет за собой применение соответствующих правовых норм.



## 641 Руководство баварского BayLfD о защите данных в процедурах закупок



Баварский орган по защите данных ("BayLfD") 27.04.2023 выпустил руководство по защите данных в контексте организации процедур закупок. Руководство описывает процедуры закупок, определяет, какие обработки персональных данных требуют внимания в процессе закупок и как с ними необходимо поступать с учетом последних решений закупочных палат и судов. Руководство разъясняет пересечения между законодательством о защите данных и законодательством о государственных закупках, подчеркивая применимые требования к облачным услугам.

## Руководство нижнесаксонского Lfd Niedersachsen по защите данных для клубов и ассоциаций



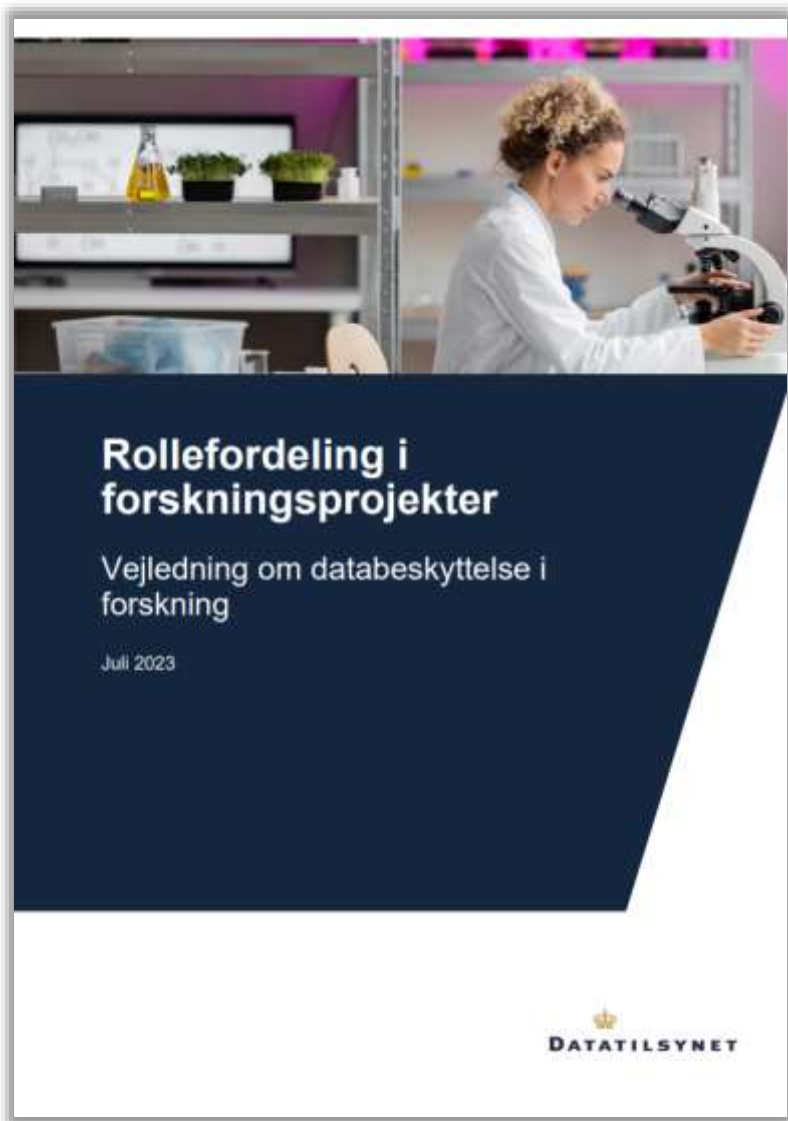
Управление по защите данных Нижней Саксонии (LfD Niedersachsen) 21.08.2023 опубликовало руководство по защите данных для клубов и ассоциаций. Руководство предназначено для клубов с различными целями, включая спорт, хобби, музыку, защиту окружающей среды и клубы самопомощи.

Во-первых, руководство рекомендует учитывать принципы обработки персональных данных в соответствии с GDPR при обработке всех персональных данных, включая прозрачность, ограничение цели, минимизацию данных, точность данных, ограничение хранения, а также целостность и конфиденциальность.

Руководство рекомендует клубам соблюдать признанную правовую основу для обработки персональных данных в соответствии с GDPR. В частности, передача персональных данных членом клуба другой организации, например, в рамках спортивного соревнования, допустима в соответствии со статьей 6(1)(b) GDPR. В руководстве поясняется, что законные интересы для обработки должны быть сбалансированы с основными правами и свободами разумных ожиданий субъектов данных, и что такое рассмотрение также применимо к данным, которые не имеют фактической связи с членами и нечленами клуба (т.е. гостями/посетителями).

О публикации информации о членах клуба, такой как результаты соревнований или выступлений, а также таких данных, как гражданство, дата рождения или адрес, которые не служат целям клуба, могут быть опубликованы только с добровольного согласия члена клуба. Руководство также рекомендует клубам разработать политику конфиденциальности с указанием типа данных, целей их обработки и того, к кому эти данные относятся, оговаривая, что пересказа положений GDPR недостаточно. Наконец, в руководстве разъясняется, что обязанность назначить ответственного за защиту данных (DPO) распространяется на клубы в соответствии с GDPR.

## 643 Руководство датского Datatilsynet по защите данных в контексте научных исследований



14.07.2023 датский орган по защите данных (Datatilsynet) опубликовал новое руководство по обработке персональных данных в контексте научных исследований. Руководство адресовано главным образом исследователям и призвано прояснить роли и обязанности различных сторон в области защиты данных.

Участники исследования могут иметь различные обязательства по защите данных в зависимости от того, считаются ли они контроллером или процессором данных в исследовательском проекте. Уровень контроля стороны над сбором и обработкой данных определяет роль стороны в области защиты данных.

В руководстве приводятся примеры ролей по защите данных, которые могут выполнять различные стороны в различных сценариях исследований:

- лица, проводящие исследования, включая студентов и научных руководителей;
- учреждения, участвующие в исследованиях, такие как университеты и больницы;
- фармацевтические компании, участвующие в клинических исследованиях;
- учреждения, продающие и передающие данные исследований.



Британский регулятор в сфере защиты персональных данных ICO (Informational Commissioner's Office) опубликовал руководство по отправке электронных писем, содержащих конфиденциальную информацию.

Поводом для создания документа стал рост случаев утечек данных из-за массовых рассылок электронных писем. Как правило, такие письма содержат персональные данные, которые попадают в публичное пространство из-за неправильного использования функций копии (Cc) и скрытой копии (Bcc) электронной почты.

Регулятор настаивает на «осторожном» использовании функции скрытой копии для того, чтобы личные адреса электронной почты не передавались другим клиентам или иным организациям.

ICO рекомендует организациям создавать политики использования сотрудниками рабочей электронной почты.

## 645 Руководство датского Datatilsynet по использованию автозаполнения в e-mail

29.08.2023 датский орган по защите данных (Datatilsynet) опубликовал руководство по обязанностям контролеров данных при использовании функции "автозаполнения" в электронных письмах. Руководство было разработано в связи с участвовавшими случаями нарушения конфиденциальности данных, вызванными отправкой пользователями электронных писем, содержащих персональные данные, неверным адресатам из-за использования функции "автозаполнения", которая заполняет адреса электронной почты получателей.

В соответствии с руководством контроллеры данных, систематически использующие электронную почту для отправки конфиденциальной и/или чувствительной информации, должны реализовать как технические, так и организационные меры для снижения риска ошибок при отправке в результате использования функции "автозаполнения":

- адреса электронной почты внешних получателей должны копироваться из CRM-системы, где они уже зарегистрированы и подтверждены;
- следует применять правило «четыре глаза», т.е. проверять электронные письма, содержащие персональные данные, перед отправкой должны два человека;
- нужно регулярно удалять сохраненные адреса электронной почты, которые не использовались в последнее время;
- следует применять функцию задержки сообщения, позволяющую удалять или редактировать письма после нажатия кнопки отправки;
- нужно использовать технические меры, предупреждающие пользователей о том, что письмо может быть отправлено неавторизованному получателю
- необходимо отключить функцию автозаполнения.

## 646 Руководство французского CNIL для фармацевтов

21.09.2023 французский орган по защите информации (CNIL) опубликовал практическое руководство для фармацевтов по защите персональных данных. В руководстве рассказывается о том, как фармацевты могут соблюдать требования GDPR, при этом фармацевты могут также опираться на справочную систему CNIL, касающуюся обработки персональных данных, предназначенных для управления аптеками.

В руководстве рассматривается вопрос о том, как аптеки могут соответствовать GDPR как при отпуске лекарств, так и при управлении аптекой:

- обстоятельства, при которых аптеке необходимо назначить ответственного за защиту данных (DPO);
- как информировать физических лиц об обработке их персональных данных и их правах;
- как внедрить процедуры, позволяющие лицам обращаться за реализацией своих прав, включая ответ на запрос о доступе к данным умершего человека;
- порядок управления отношениями с субпроцессорами, включая идентификацию субпроцессоров;
- меры, которые необходимо принять, если поставщики услуг находятся за пределами Европейского Союза, а обработка данных представляет собой их передачу;
- необходимо ли проводить оценку воздействия на защиту данных (DPIA) и каким образом.

Кроме того, в руководстве приведены типовые шаблоны для вышеуказанных активностей, например типовой шаблон для информирования субъектов данных об обработке их персональных данных и типовой шаблон для управления персональными данными сотрудников аптеки. В руководстве также указаны сроки хранения записей о персональных данных и определены меры безопасности, которые должны быть приняты для конкретных видов обработки персональных данных.

В отношении примерной практики установки видеонаблюдения в руководстве указано, что аптеки должны вести видеонаблюдение в целях безопасности зоны обращения пациентов в аптеке, сотрудников, работающих с деньгами или наркотическими веществами, которые должны храниться в запертом шкафу, а также места и запасы. Однако в руководстве отмечается, что аптекам не следует устанавливать постоянное видеонаблюдение за сотрудниками и не снимать на видео зоны отдыха и уборные.

<https://www.cnil.fr/fr/la-cnil-et-lordre-national-des-pharmaciens-publient-un-guide-rgpd>

[https://www.cnil.fr/sites/cnil/files/2023-09/guide-rgpd-cnop\\_cnil.pdf](https://www.cnil.fr/sites/cnil/files/2023-09/guide-rgpd-cnop_cnil.pdf)

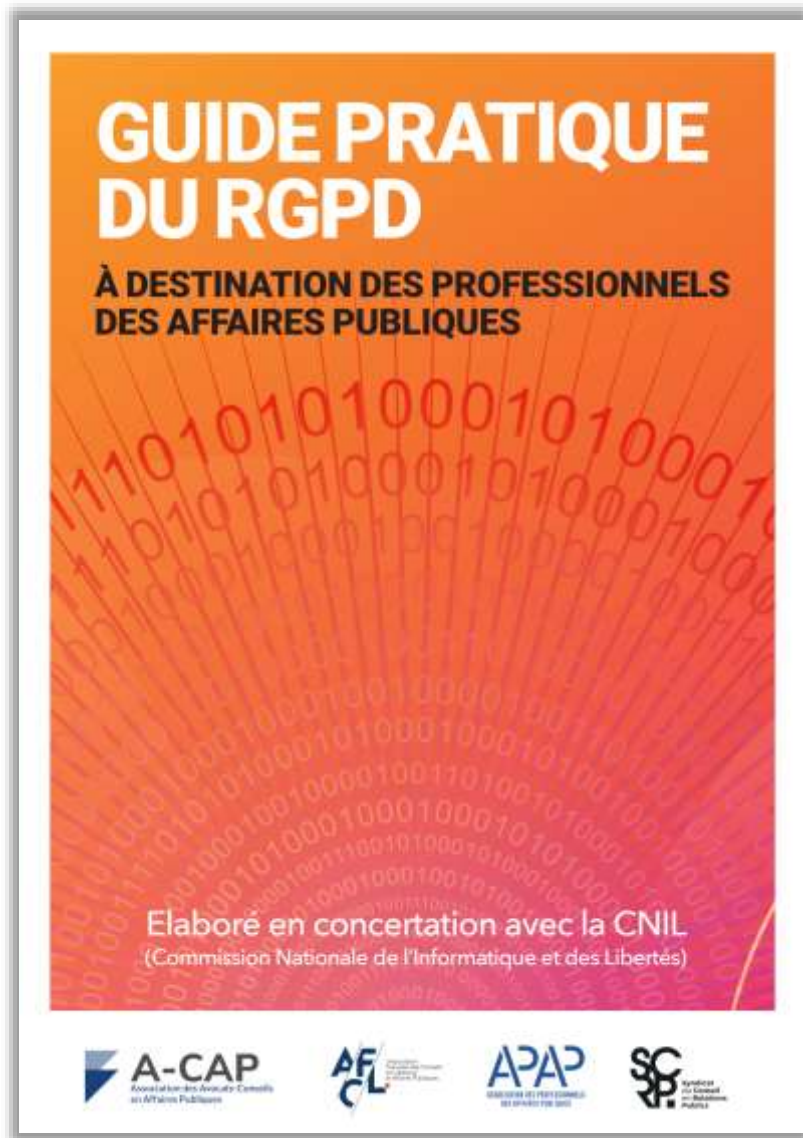


Французский орган по защите данных (CNIL) 06.03.2024 опубликовал руководство по продаже наборов для генетического тестирования. CNIL обратил внимание на большой объем собираемых персональных и конфиденциальных данных, включая информацию, связанную с геномом человека, такую как этническое происхождение, фенотипические данные и данные, касающиеся здоровья человека, а также данные, собираемые для заказа и отправки тестов, включая имена, адреса и адреса электронной почты. Кроме того, генетические данные имеют особое значение, поскольку ими делятся между собой потомки и близкие родственники.

Более конкретно, CNIL пояснил, что генетические тесты могут проводиться во Франции только для:

- судебного расследования;
- медицинского обслуживания;
- исследовательских целей.

За пределами этих обстоятельств, по мнению CNIL, необходимо получить согласие человека. Тем не менее, CNIL уточняет, что проведение генетических тестов во Франции запрещено даже с согласия соответствующего лица. Таким образом, приобретение генетического теста через Интернет жителями Франции наказывается штрафом в размере 3,750 евро, а проведение генетического теста вне медицинской и научной сферы запрещено и наказывается штрафом в размере 15,000 евро и одним годом тюремного заключения для лиц или компаний, предлагающих такие тесты.



Французский орган по защите данных (CNIL) 13.03.2024 опубликовал практическое руководство по GDPR для специалистов по связям с общественностью. Руководство предназначено для специалистов, работающих в сфере связей с общественностью, лоббирования, консалтинга, а также на внутренние отделы компаний, которые собирают персональные данные, касающиеся, в частности, представителей правительства, администраторов, парламентариев и сотрудников СМИ, в соответствии с GDPR.

Руководство может помочь специалистам по связям с общественностью:

- понять, кто является заинтересованными сторонами по тому или иному вопросу;
- взаимодействовать с указанными заинтересованными сторонами;
- поддерживать профессиональные отношения.

Руководство не охватывает операции по обработке данных, не относящиеся к деятельности государственных органов, такие как управление персоналом (HR) или коммерческое управление.



Guidance

# Ethics, Transparency and Accountability Framework for Automated Decision-Making

Updated 29 November 2023

Contents

- What the framework is for
- Understanding automated and algorithmic decision-making
- Before you use this framework
- How to use this framework
  1. Test to avoid any unintended outcomes or consequences
  2. Deliver fair services for all of our users and citizens
  3. Be clear who is responsible
  4. Handle data safely and protect citizens' interests
  5. Help users and citizens understand how it impacts them
  6. Ensure that you are compliant with the law
  7. Build something that is future proof
- Case studies
- Glossary

## What the framework is for

### Context

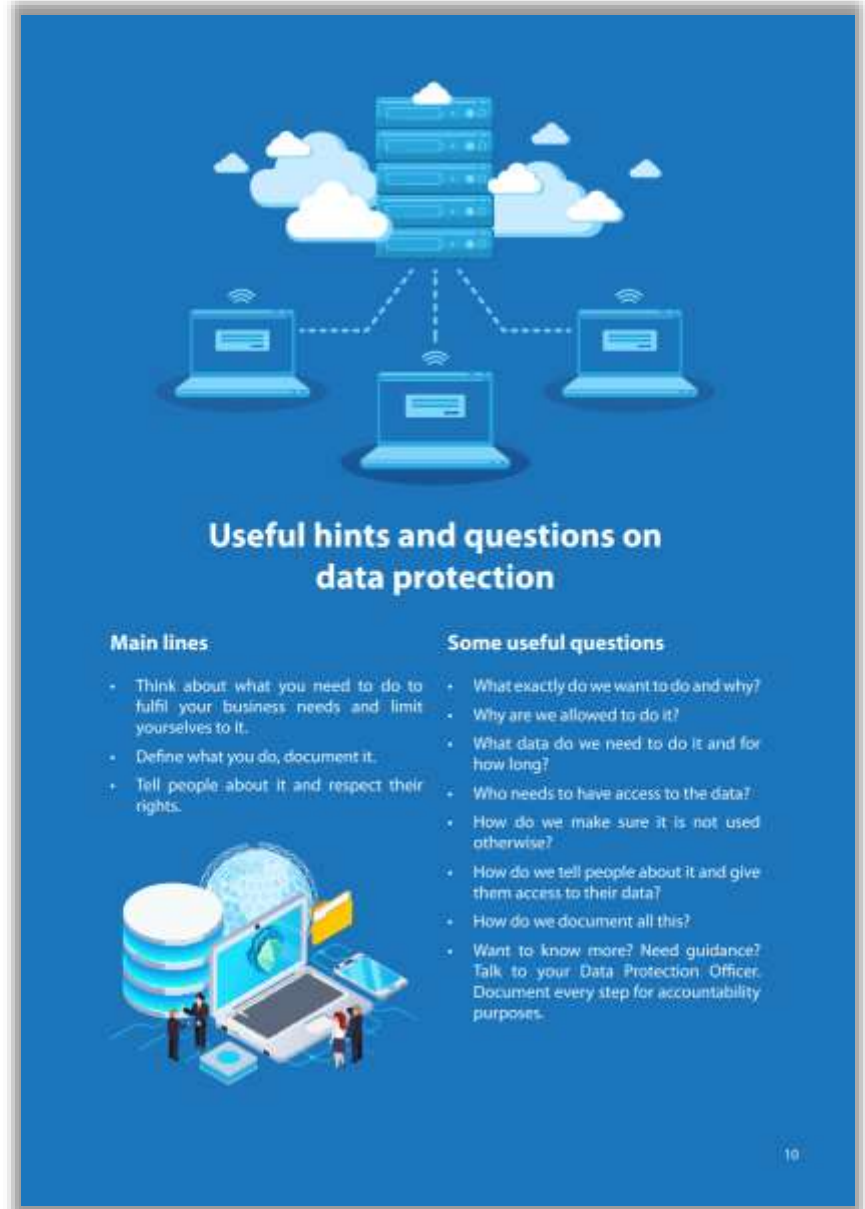
The ethical considerations of artificial intelligence and automated systems is at the centre of technological advancement.

According to a recent [EU survey](#) and a [British Computer Society survey](#) in the UK, there is a distinct distrust in the regulation of advanced technology. A [review by the Committee on Standards in Public Life](#) found that the government should produce clearer guidance on using artificial intelligence ethically in the public sector.

### Why we need the framework

Current guidance can be lengthy, complex and sometimes overly abstract. This is not just a Digital, Data and Technology issue. We need to improve the general literacy of automated or algorithmic decision-making with clear information and practical steps for civil servants and ministers to support the agenda and provide appropriate challenge.

Decision-makers should not assume that automated or algorithmic decision-making is a 'fix-all' solution, particularly for the most complex problems.



## 651 Кодекс поведения для облачных организаций



19.05.2021 EDPB опубликовал мнение «EU Data Protection Code of Conduct for Cloud Service Providers», которое позволило бельгийскому DPA утвердить этот Кодекс в качестве действующего механизма согласно ст.40 GDPR. Над Кодексом работали Alibaba Cloud, IBM, Oracle, SAP, Cisco, Google Cloud, TrustArc и другие.

«EU Cloud Code of Conduct» покрывает все виды услуг на облачном рынке (IaaS, PaaS, SaaS), но применим только для процессоров и не может быть использован в качестве механизма для трансграничной передачи. Кодекс предлагает аудируемые элементы (контроли) которые помогают добиться соответствия GDPR, а также описывает надлежащие практики работы с субпроцессорами, обеспечения безопасности данных и о многом другом.

Также была аккредитована организация, которая будет мониторить выполнение положений Кодекса всеми кто к нему присоединился.

## 652 Национальная GDPR-сертификация в Люксембурге

13.05.2022 Национальная комиссия по защите данных Люксембурга ("CNPД") утвердила «GDPR-CARPA», являющейся национальной схемой сертификации, которая не фокусируется на конкретном секторе или типе обработки. Это первая сертификационная схема в ЕС/ЕЭЗ и важный шаг в стандартизации подхода к GDPR не только в Люксембурге, но и по всей территории ЕС как European Data Protection Seal согласно ст.42 GDPR.

Использовать сертификацию можно как:

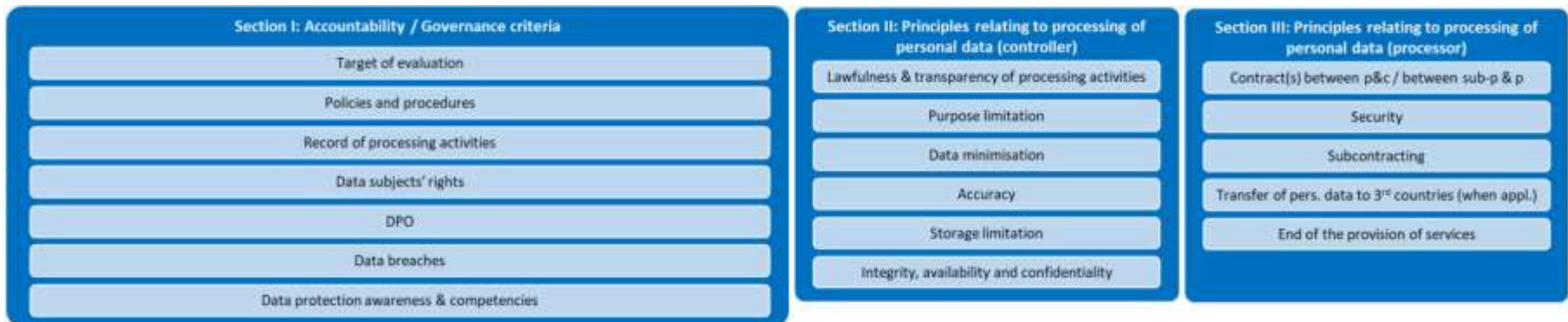
- доказательство/медаль «Мы GDPR-compliant»;
- чёткое руководство по тому, как соответствовать GDPR;
- trust-point для пользователей и бизнес-партнёров.

Сертификацию нельзя использовать:

- для международных передач по ст.46 GDPR;
- если в организации нет DPO;
- если обрабатываются данные лиц младше 16 лет;
- в рамках совместного контроля по ст.26 или в рамках ст.10 GDPR.

Ранее EDPB [просил](#) доработать GDPR-CARPA :

- унифицировать терминологию с той, что используется в GDPR;
- уточнить, кто из правления организации вправе принимать решения касательно мер по GDPR;
- указать, что DPO, несмотря на активную вовлечённость в процессе настройки системы по управлению защитой данных, не несёт ответственность за GDPR-compliance организации.



## Международные стандарты





Page [Discussion](#)

---

## Wiki for Privacy Standards and Privacy Projects

(Redirected from Wiki for Privacy Standards)

**Contents** [\[hide\]](#)

- 1 Objective of this Wiki
- 2 Content
- 3 Membership
- 4 More on IPEN - Internet Privacy Engineering Network
- 5 Sponsors and Support

[Main page](#)

[Recent changes](#)

[Wiki help](#)

---

▼ [Organisation](#)

[Contacts](#)

▶ [Standardisation](#)

▶ [Tools](#)

### Objective of this Wiki

The objective of this Wiki is to be a tool allowing stakeholders interested in privacy engineering and standardisation to find resources and to identify and seek harmonisation and convergence opportunities.

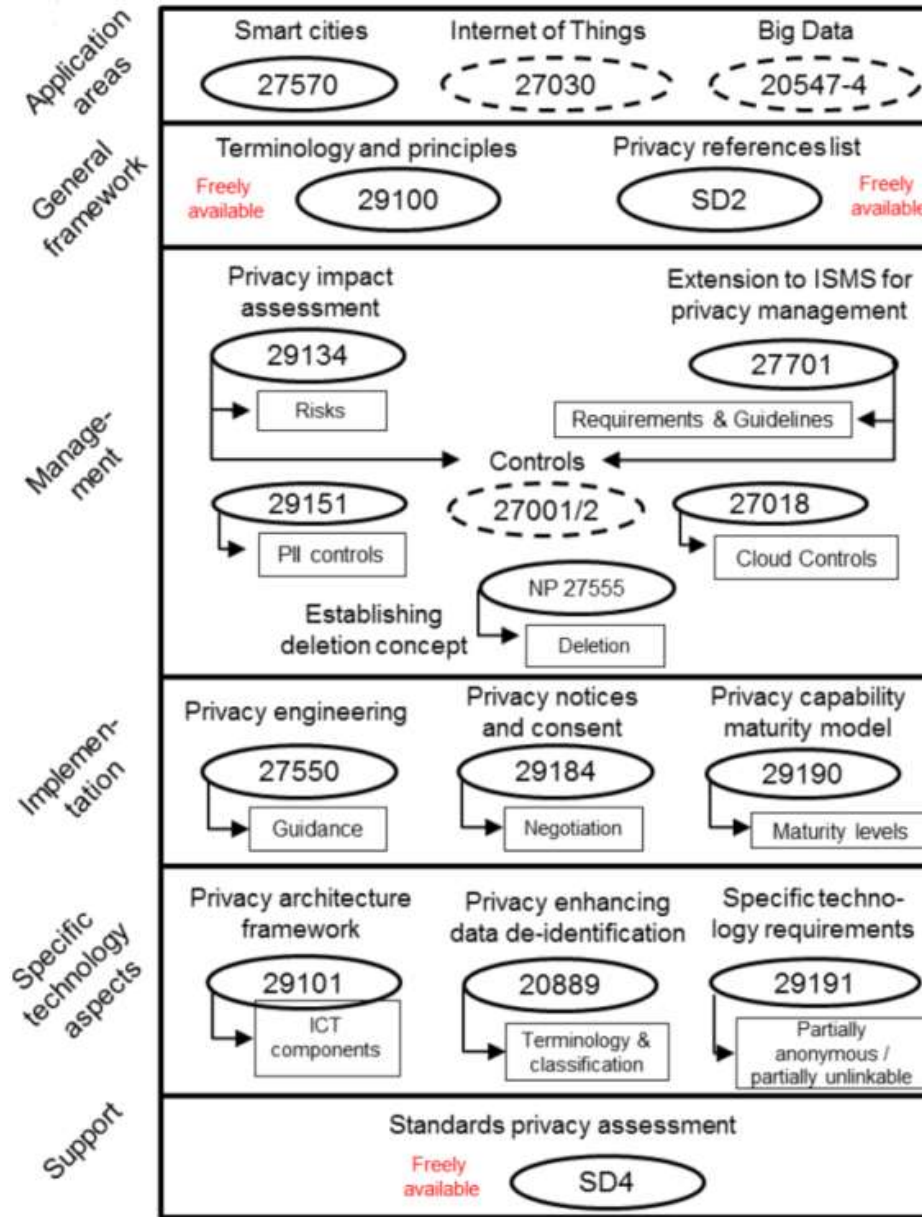
### Content

Privacy standards	Privacy engineering projects	Reports, Events, Presentations
<ul style="list-style-type: none"> <li><a href="#">CEN-CENELEC-ETSI</a></li> <li><a href="#">IETF Activities</a></li> <li><a href="#">IEEE standards</a></li> <li><a href="#">ISO/IEC</a></li> <li><a href="#">ITU standards</a></li> <li><a href="#">OASIS</a></li> <li><a href="#">OpenID Foundation</a></li> <li><a href="#">W3C Activities</a></li> <li><a href="#">National Level Standards</a></li> </ul>	<ul style="list-style-type: none"> <li><a href="#">APP Pets (ULD project)</a></li> <li><a href="#">AN.ON-Next (ULD project)</a></li> <li><a href="#">CREDENTIAL (EC project completed)</a></li> <li><a href="#">DNT Guide</a></li> <li><a href="#">PARIS (EC project completed)</a></li> <li><a href="#">PDP4E (EC project on-going)</a></li> <li><a href="#">PRIPARE (EC project completed)</a></li> <li><a href="#">PRISMACLOUD (EC project completed)</a></li> <li><a href="#">Privacy framework (NIST project on-going)</a></li> <li><a href="#">Privacypatterns</a></li> <li><a href="#">Signatu</a></li> </ul>	<ul style="list-style-type: none"> <li><a href="#">DPIA and PIA guidelines</a></li> <li><a href="#">Studies</a></li> <li><a href="#">OWASP</a></li> <li><a href="#">Business Process Cookbook</a></li> <li><a href="#">Events</a></li> <li><a href="#">Presentations</a></li> </ul>

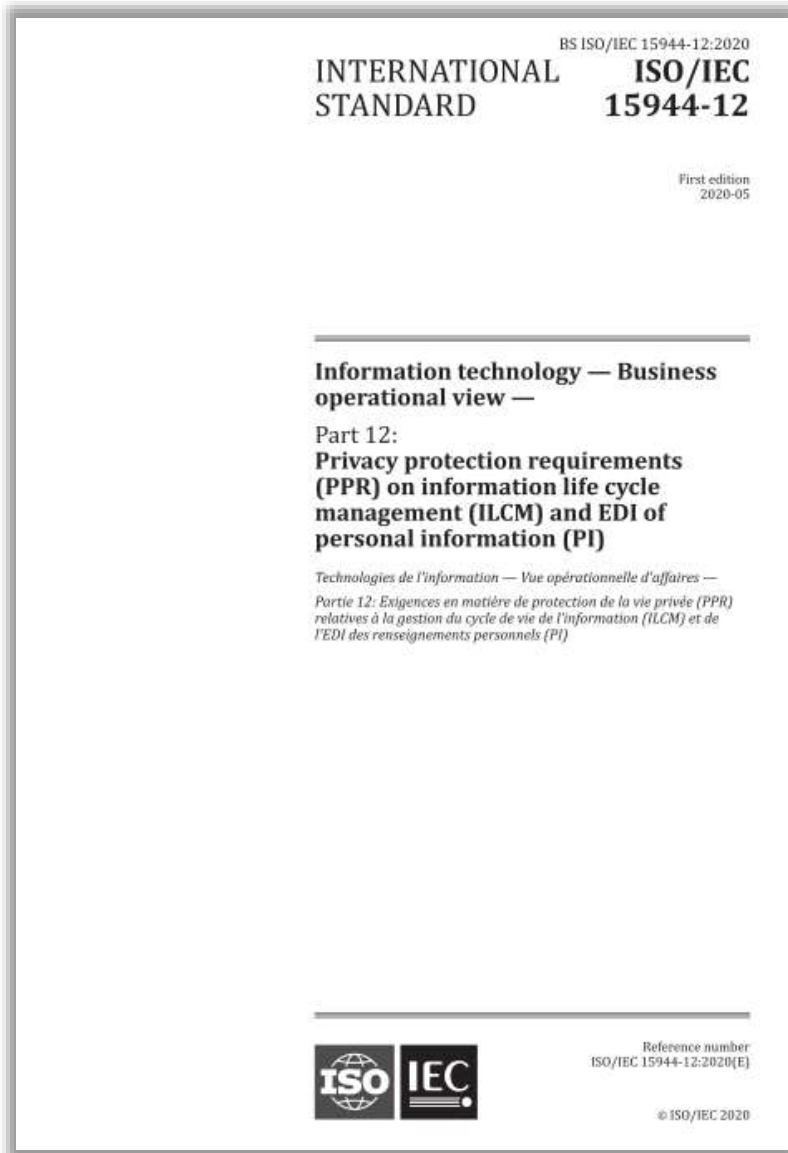
[More info on privacy standards](#) [\[Expand\]](#)

[More info on privacy engineering projects.](#) [\[Expand\]](#)

[More info on reports, events, presentations](#) [\[Expand\]](#)



## Стандарт ISO/IEC 15944-12:2020. Защита персональных данных при структурированном обмене данными

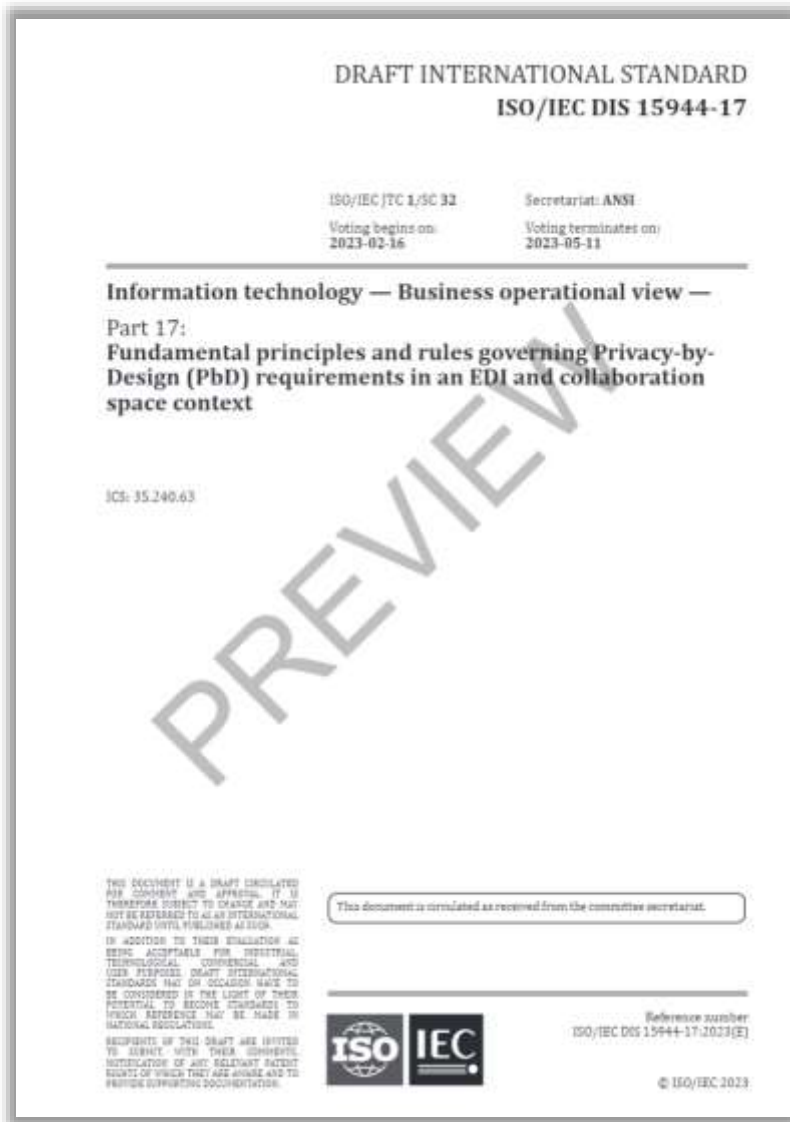


Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 15944-12:2020 «Информационные технологии – Взгляд с точки зрения деловых операций - Часть 12. Выявление требований к защите персональных данных, относящихся к управлению жизненным циклом информации и электронному EDI-обмену структурированными персональными данными» (Information technology - Business operational view - Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)).

В стандарте описаны требования по защите неприкосновенности частной жизни (privacy protection requirements, PPR) в отношении управления жизненным циклом информации (ILCM) и EDI-обмена (Electronic Data Interchange) персональными данными, представляют собой минимальный набор политик ILCM и эксплуатационных требований в отношении всей документированной информации, в особенности к той, что относится деловым транзакциям – равно как и в целом при внедрении ILCM в любой организации.



## Проект стандарта ISO/IEC 15944-17. «Запроектированная» защита персональных данных для структурированного обмена деловой информацией



Международной организацией по стандартизации (International Organization for Standardization) МЭК готовится стандарт ISO/IEC DIS 15944-17 «Информационные технологии – Оперативная точка зрения и деловую деятельность – Часть 17: Основные принципы и правила, определяющие требования к запроектированной защите персональных данных в контексте структурированного обмена информацией (EDI) и коллективной работы» (Information technology – Business operational view – Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space context).

Стандарт обращает особое внимание на аспекты обеспечения «запроектированной» защиты персональных данных (Privacy by design, PbD) в требованиях по защите неприкосновенности частной жизни (персональных данных), - в качестве внешних ограничений для лица любого типа (например, организации или государственной администрации), вовлеченного в деловые транзакции любого вида между такими лицами, которые включает электронный обмен (electronic data interchange, EDI) какими-либо персональными данными..

## Технические спецификации ISO/IEC TS 17975:2022. Принципы и требования к данным для согласия на сбор, использование или раскрытие персональной информации о здоровье



Документ определяет набор концептуальных рамок для управления согласиями на сбор, использование и/или раскрытие персональной информации практикующими врачами и организациями, которые часто используются для получения согласия на обработку персональной информации о здоровье субъектов ухода.

Целью документа является формулирование концепции информированного согласия (informational consent), которая может быть специфицирована и использована в отдельных областях регулирования (например, организациями здравоохранения, региональными органами здравоохранения, юрисдикциями, странами) в качестве помощи в согласованном управлении информацией при предоставлении медицинских услуг и при передаче электронных медицинских документов через границы организаций и юрисдикций. Данный документ применим в отношении персональной информации о здоровье (Personal Health Information, PHI).

Требования хорошей практики специфицированы для каждой из рамок использования информированного согласия. Соблюдение этих требований должно обеспечить уверенность субъектов ухода и всех обрабатывающих персональную информацию о здоровье сторон в том, что согласие на такую обработку было получено надлежащим образом и правильно сформулировано.



Международной организацией по стандартизации (International Organization for Standardization) был опубликован технический отчёт ISO/IEC TR 20322:2023 «Информационные технологии - Транс-юрисдикционные и социальные аспекты внедрения биометрических технологий - Биометрия и люди пожилого возраста» (Information technology - Cross-jurisdictional and societal aspects of implementation of biometric technologies - Biometrics and elderly people).



Международной организацией по стандартизации (International Organization for Standardization) были опубликованы технические спецификации ISO/IEC TS 20748-4:2019 «Информационные технологии для обучения, образования и подготовки - Интероперабельность средств сбора и обработки данных об учащихся - Часть 4: Политики защиты неприкосновенности частной жизни и защиты персональных данных» (Information technology for learning, education and training - Learning analytics interoperability - Part 4: Privacy and data protection policies).

В документе устанавливаются требования к защите неприкосновенности частной жизни и персональных данных, которые должны использоваться при проектировании систем сбора и обработки данных об учащихся (learning analytics) и в практике сбора и обработки такого рода данных в школах, университетах, при обучении на рабочем месте и при использовании смешанных подходов к обучению.

## 661 Стандарт ISO/IEC 20889:2018. Обезличивание персональных данных



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 20889:2018 «Терминология и классификация методов де-идентификации (обезличивания) данных с целью усиления защиты неприкосновенности частной жизни (персональных данных)» (Privacy enhancing data de-identification terminology and classification of techniques).

В стандарте описаны усиливающие защиту неприкосновенности частной жизни методы де-идентификации данных. Стандарт предназначен для использования при описании и проектировании мер по де-идентификации в соответствии с принципами защиты неприкосновенности частной жизни, сформулированными в стандарте ISO/IEC 29100:2011 «Информационная технология. Методы и средства обеспечения безопасности. Концепция защиты персональных данных» (Information technology - Security techniques - Privacy framework).



Международной организацией по стандартизации (International Organization for Standardization) был опубликован технический отчет ISO/IEC TR 24028:2020 – Информационные технологии. Искусственный интеллект. Обзор вопросов доверия к искусственному интеллекту (Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence). отчет описывает практические решения для повышения доверенности систем, предоставляющих собой или использующих технологии искусственного интеллекта, а также предназначен для организаций любого размера и сферы деятельности. Документ направлен на то, чтобы оказать содействие в установлении заданного уровня доверия к системам ИИ путем повышения их прозрачности и объяснимости, снижения рисков и угроз, связанных с ошибками проектирования ИИ, и обеспечения доступности, отказоустойчивости и точности систем ИИ. Кроме того, отчет охватывает такие смежные области как взаимодействие с заинтересованными сторонами, тестирование и вопросы предвзятости ИИ.

## 663 Стандарт ISO/IEC 24745:2022. Безопасность и защита биометрических данных



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27745:2022 «Защита данных с помощью биометрии – востребованный метод обеспечения информационной безопасности» (Information security, cybersecurity and privacy protection — Biometric information protection).

В стандарте также представлены требования и рекомендации по безопасному управлению и обработке биометрической информации с соблюдением требований конфиденциальности. Темы, затрагиваемые в документе, включают:

- анализ угроз и мер защиты, типичных для биометрических систем;
- требования безопасности при привязке биометрических данных к конкретной личности;
- руководство по защите конфиденциальности в ходе обработки биометрической информации.

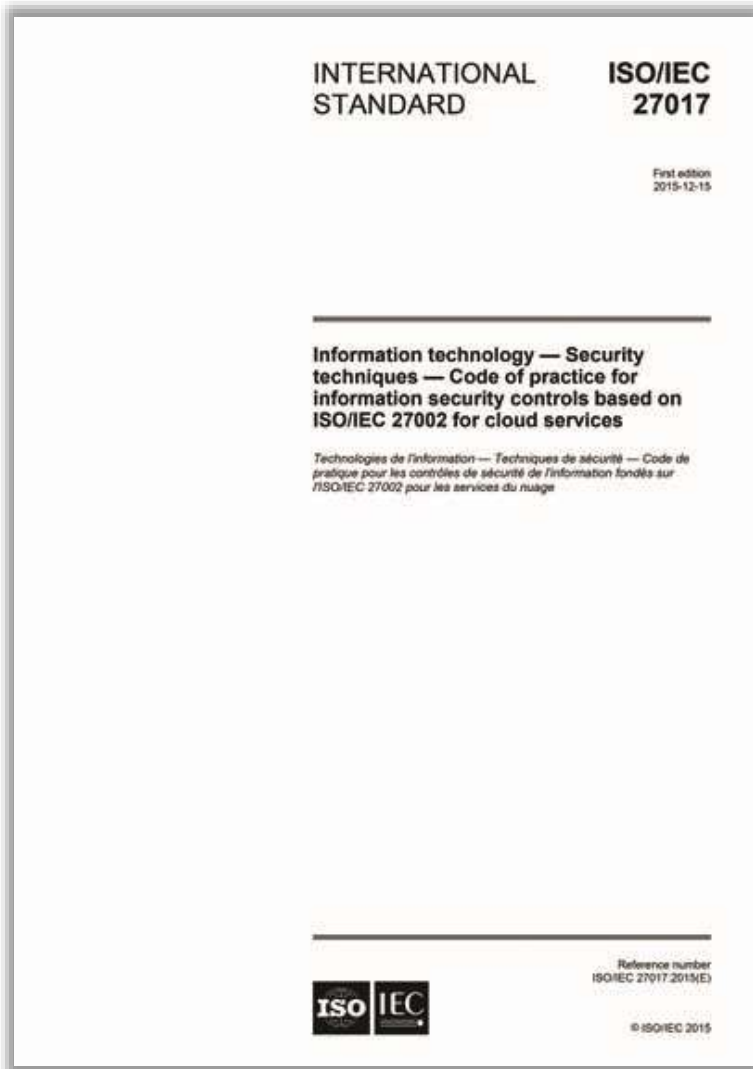
## Стандарт ISO/IEC 27001:2022. Система менеджмента информационной безопасности



Международной организацией по стандартизации (International Organization for Standardization) опубликован стандарт ISO/IEC 27001:2022 «Информационные технологии - Методы обеспечения безопасности - Системы Менеджмента Информационной Безопасности - Требования» (Information technology - Security techniques - Information security management systems - Requirements). Содержит требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности (СМИБ). В собраны описания лучших мировых практик в области управления информационной безопасностью. Стандарт устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы. Настоящий стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения Системы Менеджмента Информационной Безопасности (СМИБ).



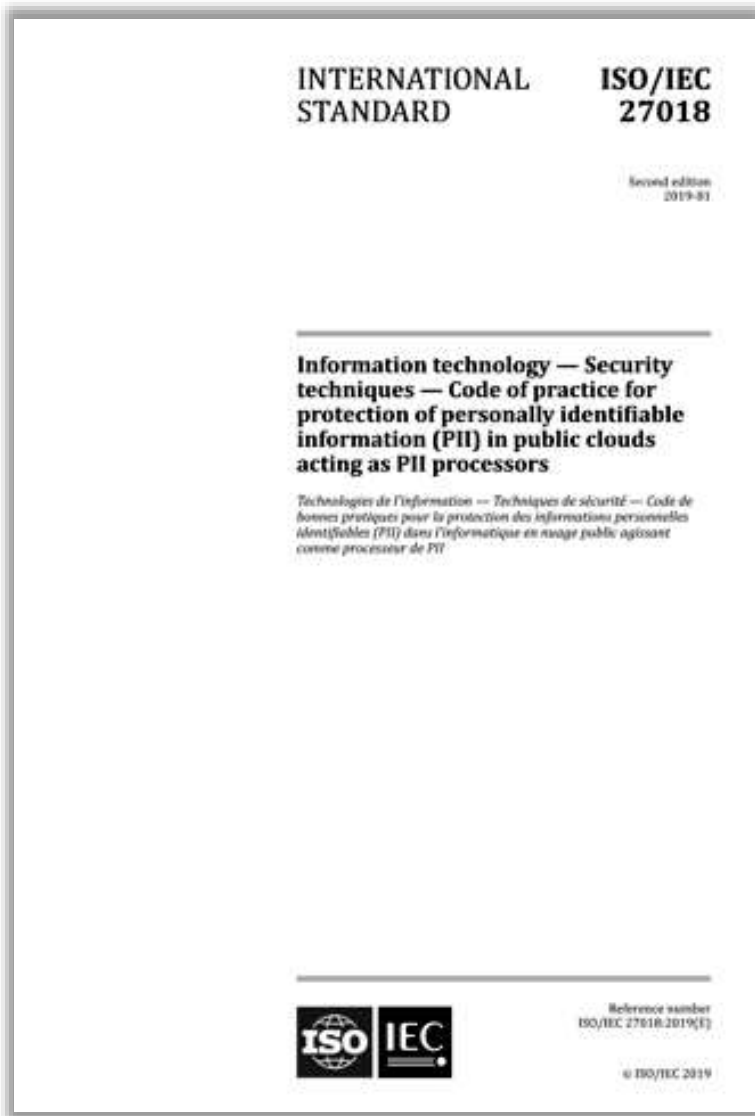
## Стандарт ISO/IEC 27017:2015. Защита персональных данных при предоставлении облачных услуг



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27017:2015 «Информационные технологии - Методы обеспечения безопасности - Система менеджмента облачной безопасности и защиты персональных данных - Меры безопасности» (Information technology - Security techniques - Cloud computing security and privacy management system - Security controls).

Стандарт содержит указания по мерам обеспечения информационной безопасности, применимым при предоставлении и использовании облачных услуг, в том числе за счет дополнительных рекомендаций по внедрению соответствующих мер, перечисленных в стандарте ISO/IEC 27002, а также дополнительных, специфических для облачных сервисов мер контроля и управления, а также рекомендаций по их внедрению. Стандарт предлагает меры контроля и управления, а также рекомендации по их внедрению как поставщикам облачных услуг, так и их клиентам.

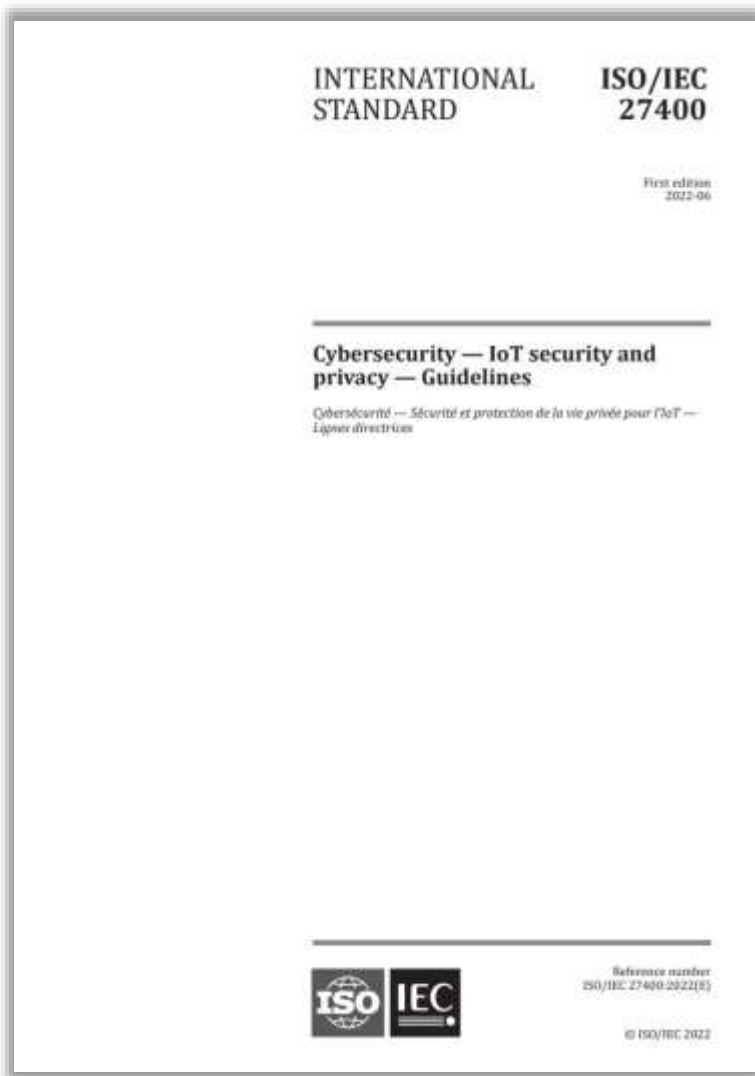
## Стандарт ISO/IEC 27018:2019. Практика защиты персональных данных в публичных облаках



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27018:2019 «Информационные технологии - Методы обеспечения безопасности - Практика защиты персональных данных в публичных облаках, выступающих в роли обработчиков персональных данных» (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).

Стандарт устанавливает общепринятые цели управления, меры и средства управления и даёт рекомендации по реализации мер по защите персональных данных (Personally Identifiable Information, PII) в соответствии с принципами защиты неприкосновенности частной жизни, сформулированными в стандарте ISO/IEC 29100, для среды облачных вычислений в публичных облаках.

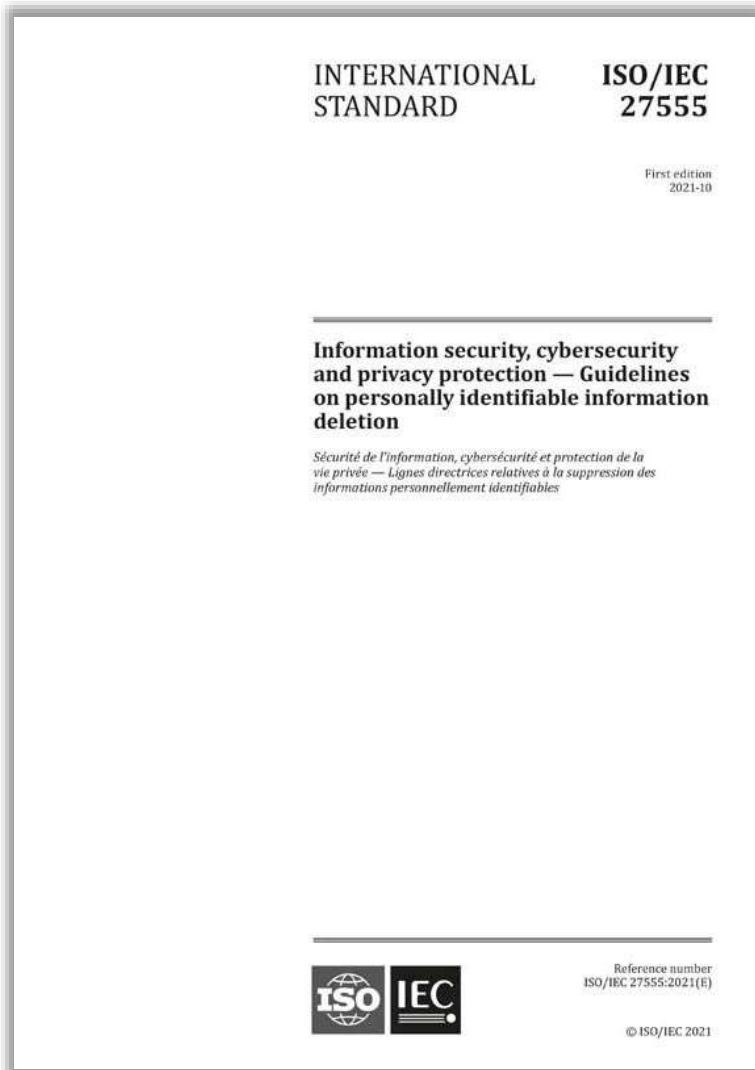
## Стандарт ISO/IEC 27400:2022. Безопасность и защита неприкосновенности частной жизни в рамках интернета вещей



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27400:2022 «Кибербезопасность – Безопасность и защита неприкосновенности частной жизни в рамках интернета вещей – Руководство» (Cybersecurity – IoT security and privacy – Guidelines).

Стандарт предлагает меры и средства контроля и управления для обеспечения безопасности и защиты персональных данных разработаны для заинтересованных сторон в среде IoT-систем, так, чтобы они могли быть использованы любой заинтересованной стороной на протяжении всего жизненного цикла IoT-системы. В документе содержатся рекомендации по рискам, принципам и мерам безопасности и защиты персональных данных для решений интернета вещей (IoT).

## Стандарт ISO/IEC 27555:2021. Руководство по уничтожению персональных данных

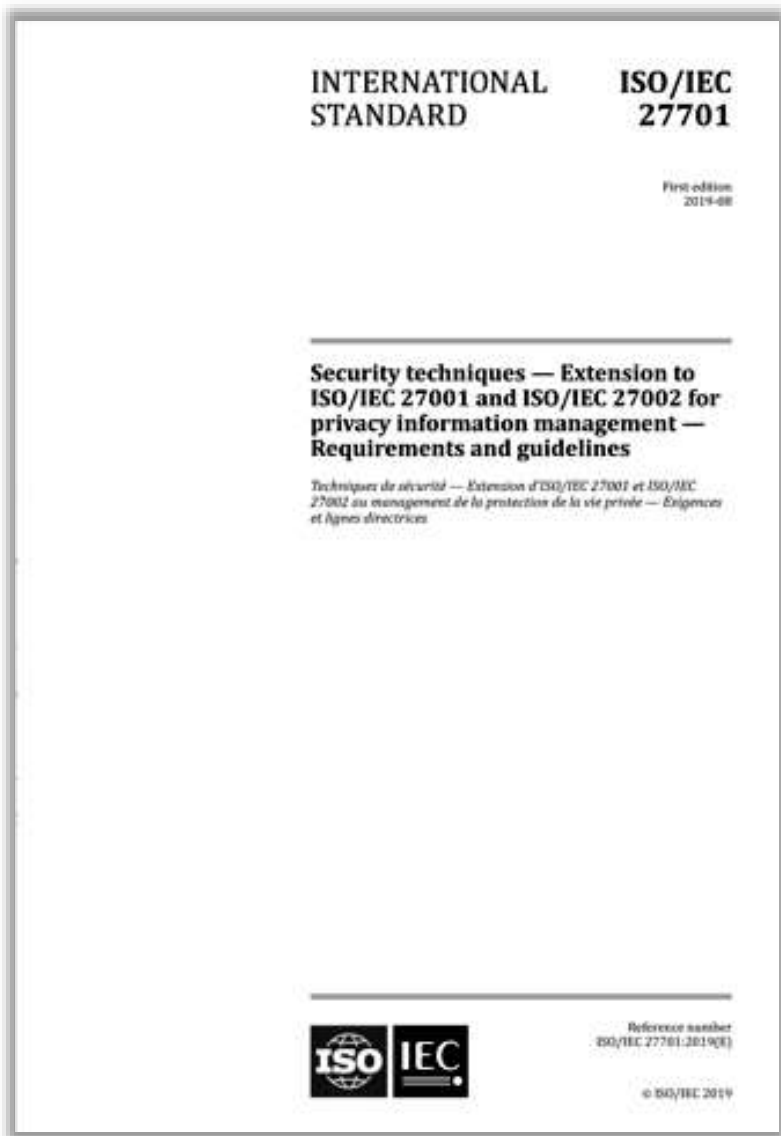


Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC ISO/IEC 27555:2021 «Информационная безопасность, кибербезопасность и защита неприкосновенности частной жизни - Руководство по уничтожению персональных данных» (Information security, cybersecurity and privacy protection - Guidelines on personally identifiable information deletion).

Он был подготовлен на основе немецкого стандарта DIN 66398:2016-05 «Руководство по разработке политики установления сроков хранения и уничтожения персональных данных» (Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten).

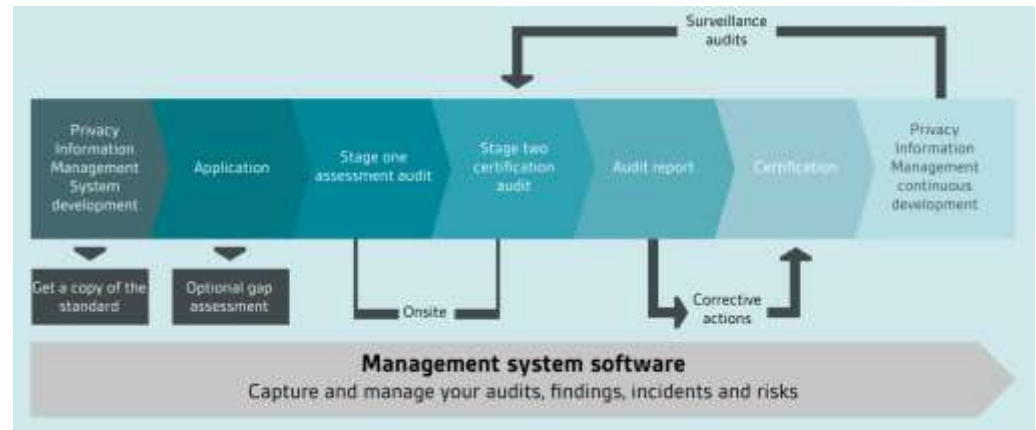
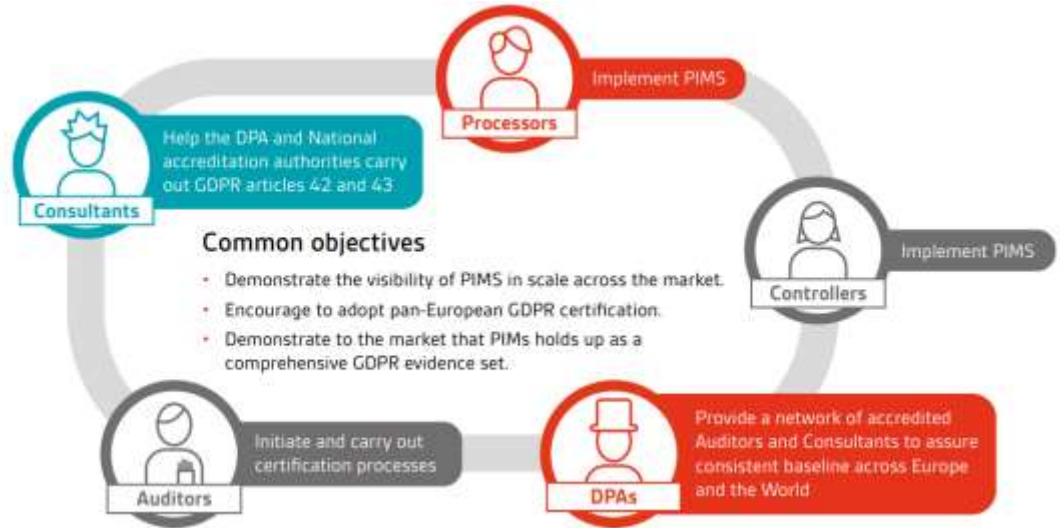
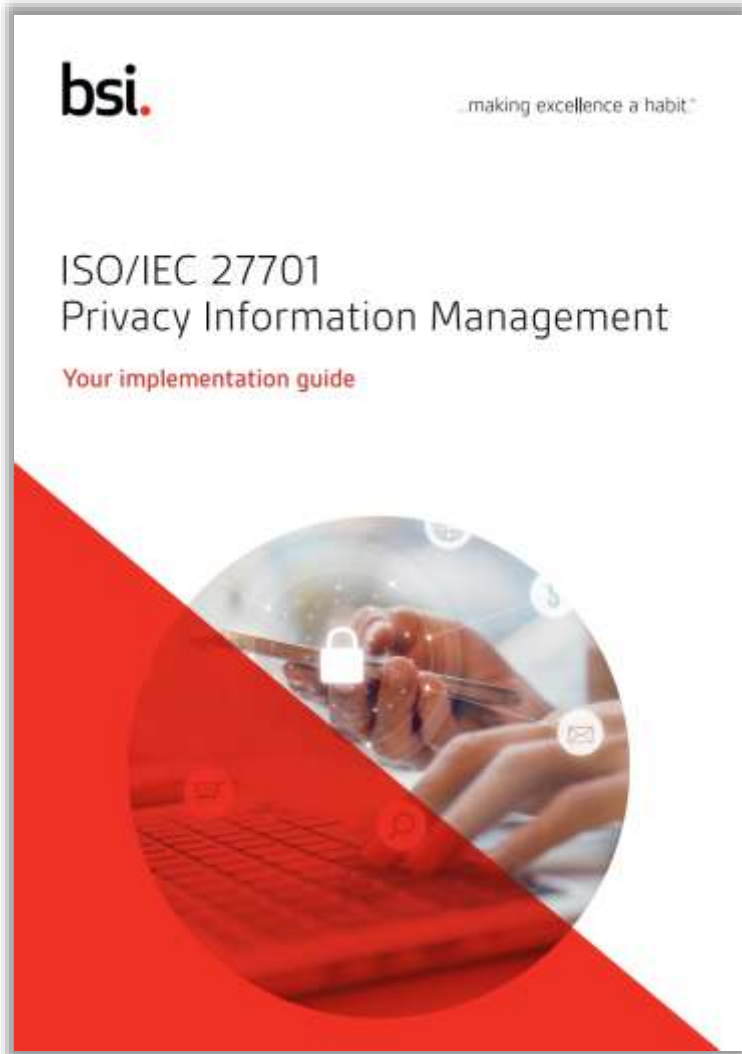
Стандарт предлагает концепцию разработки и реализации политик и процедур уничтожения персональных данных, которая может быть внедрена в организации. В документе содержатся рекомендации по разработке и реализации политик и процедур уничтожения персональных данных, описывающие гармонизированную терминологию в области уничтожения персональных данных, метод эффективного установления правил уничтожения, необходимую документацию и общее определение ролей, обязанностей и процессов.

## Стандарт ISO/IEC 27701:2019. Расширение до ISO/IEC 27001 и ISO/IEC 27002 по управлению персональными данными



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт 27701:2019 «Методы обеспечения безопасности - Расширение до ISO/IEC 27001 и ISO/IEC 27002 по управлению персональными данными - Требования и руководящие указания» (Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines).

В стандарте описано руководство по созданию, внедрению, поддержанию и постоянному совершенствованию Системы управления персональными данными (Privacy Information Management System - PIMS) в контексте организации. Стандарт определяет требования, связанные с PIMS, и формулирует правила для контролеров (controllers) и обработчиков (processors) в отношении обработки персональных данных.





**Privacy Information Management with ISO 27701**

Patrick Soenen, Partner, Qualified Audit Academy

**GDPR**

The application of the **General Data Protection Regulation (GDPR)** on 25th May 2018 means that all organisations, wherever they are established, must now comply with this regulation if they process the personal data of EU citizens. Therefore, an organisation must carefully consider how to handle the personal information of customers, employees and visitors. However, the regulation doesn't provide much guidance on what the measures to protect personal data should look like.



**Overview of the ISO 27701**

The ISO/IEC 27701:2019 standard is the first international privacy standard, which outlines the requirements for implementing a **Privacy Information Management System (PIMS)**, to govern the handling of personal data, called Personally Identifiable Information (PII) in ISO 27701.

Who should implement ISO 27701?

ISO 27701 has been designed to be used by all data controllers and data processors. Like ISO 27001, it advocates a risk-based approach so that each conforming organisation addresses the specific risks it faces, as well as the risks to personal data and privacy.



GDPR certification

While ISO 27701 is not yet governed by accreditation bodies, it is expected that certification bodies will begin to audit against this new ISO standard despite no established scheme has yet been defined at the International Accreditation Forum (IAF) level.



ISO 27701 - an extension to ISO 27001

Since many organisations already have an ISO 27001 ISMS, it reduces the complexities around establishing a Privacy Information Management System (PIMS), since the ground has already been laid. Those organisations familiar with ISO 27001 will be able to extend their ISMS to address privacy and support them in GDPR compliance by providing a means to demonstrate commitment to privacy information management.

Terminology differences between GDPR and ISO 27701

ISO/IEC 27701:2019 uses the vocabulary common to the suite of ISO 2700x standards that cover information security and associated controls. It uses the term Personally Identifiable Information (PII) to describe the information assets that must be protected and managed when providing security and privacy for a data subject, called PII principal.

The major differences in terminology between the ISO 27701 standard and GDPR are outlined in the table below:

ISO 27701	GDPR
<b>Personally identifiable information (PII)</b>	Personal data
<b>PII controller</b>	Data controller
<b>PII processor</b>	Data processor
<b>Joint PII controller</b>	Joint controller
<b>PII principal</b>	Data subject
<b>Privacy by design</b>	Data protection by design
<b>Privacy by default</b>	Data protection by default

To make this publication easier to read, we have replaced the above ISO 27701 terms by the GDPR terminology.

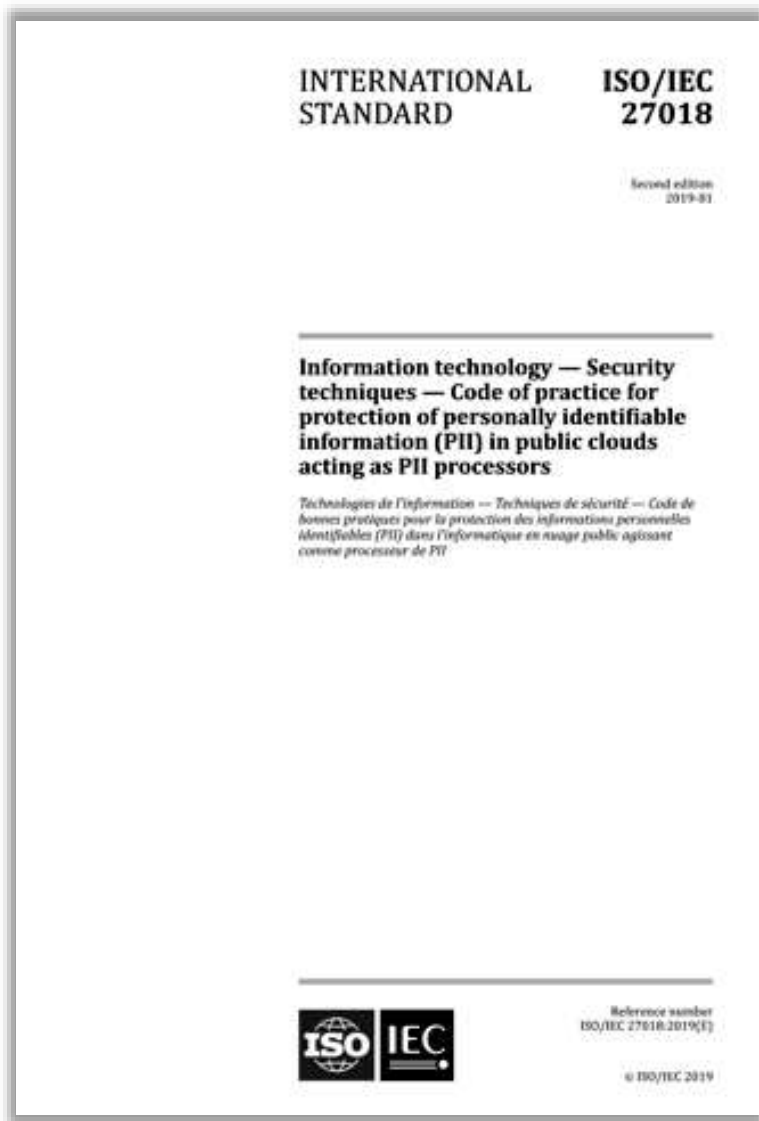
Information security

Adequate information security is necessary for privacy of personal data but is not enough by itself. Preventing the disclosure, loss or corruption of personal data cannot be effective unless the entire life cycle of the personal data processing is protected through information security controls. The ISO standard defines information security as the result of adequate controls to preserve the confidentiality, integrity and availability of information.

Good practice supports the identification of control objectives to address privacy risks. One privacy risk might apply to more than one privacy control objective. Each control objective requires the design of a suite of controls – some organisational,



## 672 Стандарт ISO/IEC 27102:2019. Руководство по киберстрахованию



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27102:2019 «Менеджмент информационной безопасности - Руководство по киберстрахованию» (Information security management - Guidelines for cyber-insurance).

Стандарт устанавливает рекомендации относительно того, когда имеет смысл рассмотреть вопрос о приобретении киберстраховки в качестве варианта обработки риска при менеджменте воздействия киберинцидента в рамках используемой организацией системы менеджмента рисков информационной безопасности.



## Стандарт ISO/IEC TR 27750:2019. Инженерия обеспечения неприкосновенности частной жизни

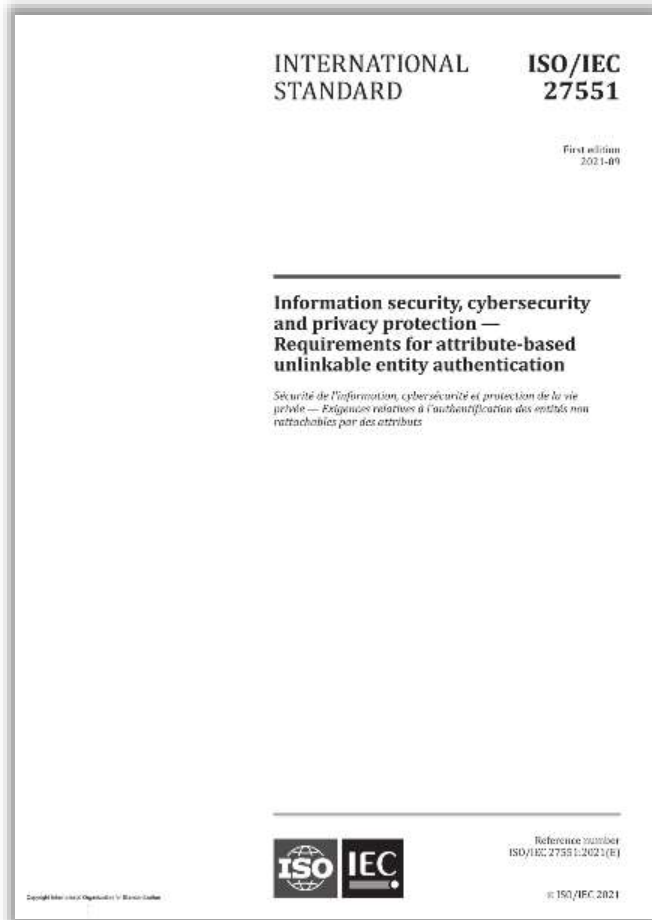


Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт 27750:2019 «Информационная безопасность - Меры безопасности - Инженерия обеспечения неприкосновенности частной жизни» (Information technology - Security techniques - Privacy engineering).

В стандарте описаны рекомендации по спроектированной защите неприкосновенности частной жизни (privacy engineering), которые призваны помочь организациям интегрировать последние достижения в сфере такого рода «встроенной» защиты в их практику проектирования систем:

Документ описывает взаимосвязь между инженерией защиты неприкосновенности частной жизни и другими инженерными точками зрения (системное проектирование, инженерия безопасности, управление рисками), а также описывает инженерию защиты неприкосновенности частной жизни в числе ключевых по важности процессов проектирования, таких, как управление знаниями, управление рисками, анализ требований, проектирование архитектуры.

## Стандарт ISO/IEC 27551:2021. Требования к основанной на атрибутах несвязываемой аутентификации объектов



Основанная на атрибутах несвязываемая аутентификация объектов (attribute-based unlinkable entity authentication, ABUEA) предоставляет субъектам ПДн средства для установления аутентичности избранного подмножества атрибутов из их идентификационного профиля, без раскрытия большего подмножества. Особое внимание уделяется обеспечению несвязываемости, и вводится метрика, которая измеряет силу этого свойства в реализациях ABUEA. В данном документе особое внимание обращается на ситуации, когда как минимум бы один атрибут подтверждается третьей стороной. В данном документе также выделяются свойства безопасности, которые необходимо реализовать для обеспечения защиты различного рода, а также свойства несвязываемости.

Разработанная в данном документе методология может быть адаптирована и применена в отношении других принципов обеспечения неприкосновенности частной жизни. Сформулированные в данном документе требования применяются на уровне информационного обмена с приложением (application communication layer). Однако некоторые свойства, реализованные в протоколе прикладного уровня, могут быть нарушены протоколом более низкого уровня (например, сетевого), - и это означает, что свойства протоколов нижних уровней, связанные с обеспечением безопасности и неприкосновенности частной жизни, также должны быть приняты во внимание для того, чтобы обеспечить, чтобы свойства реализованные на уровне информационного обмена с приложением сохранялись при рассмотрении характеристик нижележащих коммуникационных уровней, касающихся обеспечения безопасности и неприкосновенности частной жизни.

## Стандарт ISO/IEC 27556:2022. Ориентированная на пользователя концепция управления предпочтениями в плане обеспечения неприкосновенности частной жизни



В настоящем документе описывается ориентированная на пользователя концепция обработки персональных данных на основе предпочтений в плане обеспечения неприкосновенности частной жизни и их администрирования в информационно-коммуникационных (ИКТ) системах.

В обрабатывающих персональные данные ИКТ-системах реализуются механизмы контроля и управления для обеспечения неприкосновенности частной жизни. Чтобы внедрить эффективные механизмы контроля и управления для обеспечения неприкосновенности частной жизни в ИКТ-системах, контроль над персональными данными осуществляется с использованием соответствующих предпочтений, установленных (прямо или косвенно) соответствующим субъектом персональных данных, включая сведения о согласии.

Данный документ можно использовать:

- для разработки и внедрения ИКТ-систем, которые обрабатывают персональные данные или передают их между организациями;
- для разработки платформ обмена персональными данными на основе предпочтений в плане обеспечения неприкосновенности частной жизни;
- для предоставления услуги по управлению предпочтениями в плане обеспечения неприкосновенности частной жизни.

## Стандарт ISO/IEC 27557:2022. Менеджмент в организации риска, связанного с неприкосновенностью частной жизни



Данный стандарт предлагает концепцию оценки риска организации, связанного с обеспечением неприкосновенности частной жизни, с учётом соответствующего воздействия на отдельных лиц в качестве компоненты общего риска организации. Настоящий документ содержит рекомендации по менеджменту в организации риска, связанного с неприкосновенностью частной жизни.

Документ предлагает организациям рекомендации по интеграции рисков, связанных с обработкой персональных данных, в рамках программы организации по менеджменту рисков, связанных с неприкосновенностью частной жизни. В нём проводится различие между воздействием на отдельного человека, которое может повлечь обработка ПДн, и последствиями для организаций (например, репутационный ущерб), и даются рекомендации по включения в совокупную оценку рисков организации следующего:

- последствий для организации вследствие неблагоприятного воздействия на неприкосновенность частной жизни отдельных лиц;
- последствия для организации вследствие нарушений, связанных с неприкосновенностью частной жизни (privacy events), которые наносят ущерб организации (например, вредя её репутации), хотя при этом не влекут каких-либо неблагоприятных последствий для неприкосновенности частной жизни отдельных лиц.

## Стандарт ISO/IEC 27559:2022. Концепция обезличивания данных, способствующего усилению защиты неприкосновенности частной жизни



Документ предлагает организациям концепцию внедрения, обеспечивающую стратегическое управление надлежащим использованием методов де-идентификации данных, описанных в стандарте ISO/IEC 20889 «Терминология и классификация методов де-идентификации (обезличивания) данных с целью усиления защиты неприкосновенности частной жизни (персональных данных)» (Privacy enhancing data de-identification terminology and classification of techniques).

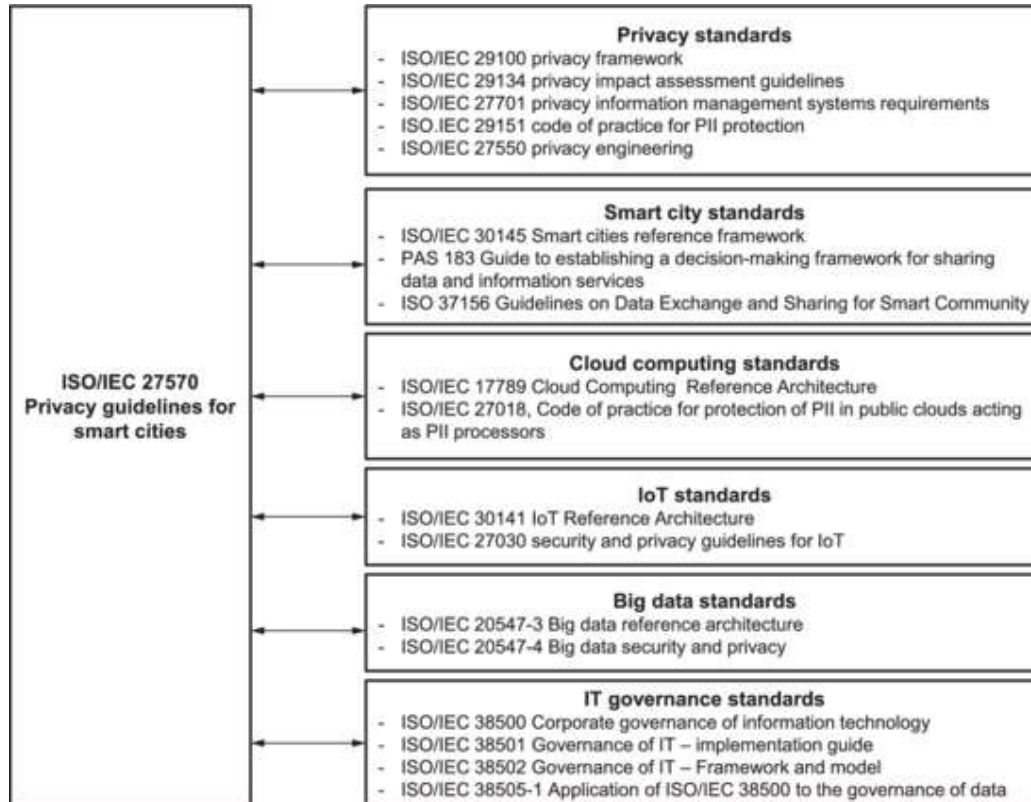
Эта концепция де-идентификации может применяться на всех этапах жизненного цикла данных: от разработки средств сбора данных до внутреннего повторного использования этих данных, предоставления данных внешним партнерам и архивации данных. Таким образом, получатели данных могут быть внутренними или внешними сторонами по отношению к ответственному хранителю данных, который внедряет процедуры и методы в соответствии с данной концепцией де-идентификации.

Данный документ применим в организациях любого типа и размера, включая государственные и частные компании, государственные учреждения и некоммерческие организации, которые являются операторами ПДн либо их обработчиками, действующими от имени оператора, и выполняют процессы де-идентификации данных для целей усиления защиты неприкосновенности частной жизни.

<https://www.iso.org/standard/71677.html>

<https://iapp.org/news/a/a-new-standard-for-anonymization/>

## Технические спецификации ISO/IEC TS 27570:2021. Защита неприкосновенности частной жизни для умных городов



Международной организацией по стандартизации (International Organization for Standardization) были опубликованы технические спецификации ISO/IEC TS 27570:2021 «Защита неприкосновенности частной жизни – Руководство по защите неприкосновенности частной жизни для умных городов» (Privacy protection – Privacy guidelines for smart cities).

В документе содержатся рекомендации по следующим вопросам:

- защита неприкосновенности частной жизни в экосистеме умного города;
- как стандарты могут использоваться на глобальном уровне и на уровне отдельной организации на благо граждан;
- процессы защиты неприкосновенности частной жизни в экосистеме умного города.

Стандарт применим в организациях любого типа и размера, включая государственные и частные компании, государственные учреждения и некоммерческие организации, которые оказывают услуги в среде умного города.

## Стандарт ISO/IEC 29100:2024. Концепция защиты персональных данных



Международной организацией по стандартизации (International Organization for Standardization) был разработан стандарт 29100:2024 «Информационная технология. Методы и средства обеспечения безопасности. Концепция защиты персональных данных» (Information technology - Security techniques - Privacy framework).

В стандарте сформулированы принципы и меры по защите неприкосновенности частной жизни. В России адаптирована как ГОСТ Р ИСО/МЭК 29100-2021 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности» предыдущая версия этого стандарта от 2018г.

## Стандарт ISO/IEC 29101:2018. Концепция архитектуры, обеспечивающая защиту персональных данных

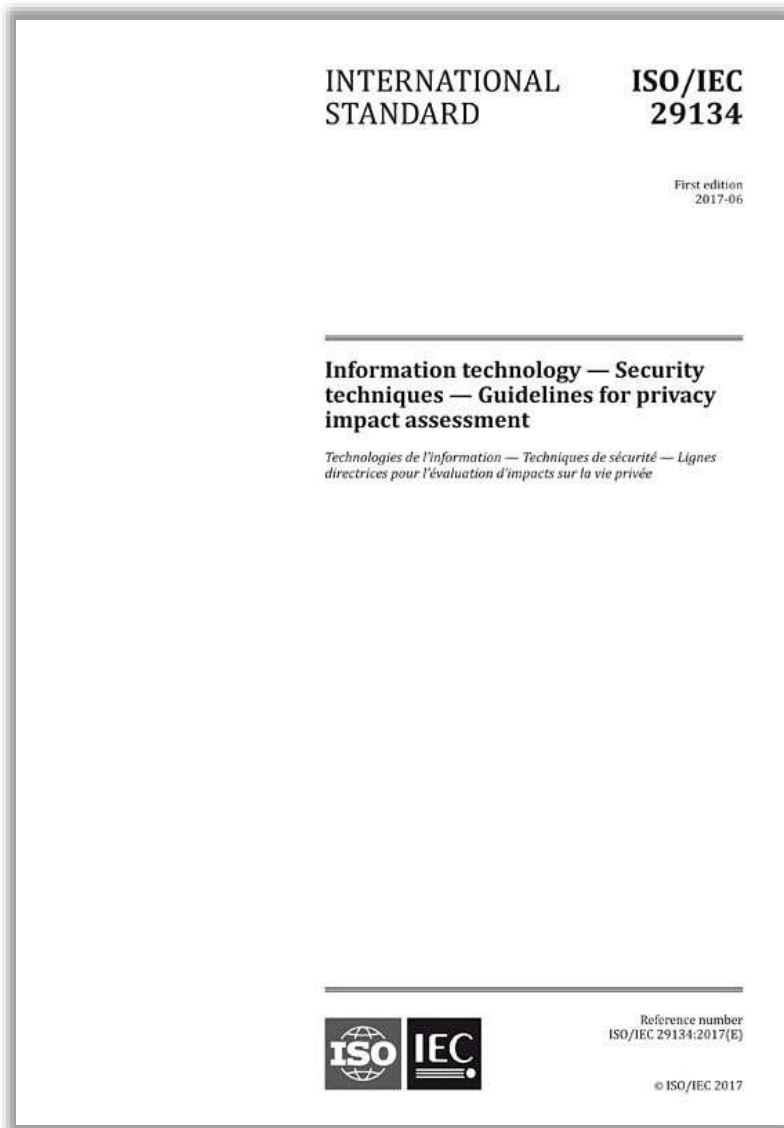


Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 29101:2018 «Информационная безопасность – Меры безопасности – Концепция архитектуры, обеспечивающей защиту персональных данных» (Information technology - Security techniques - Privacy architecture framework).

В стандарте описаны высокоуровневая концепция архитектуры и взаимосвязанные с ней меры контроля и управления, используемые для защиты неприкосновенности частной жизни (персональных данных) в ИКТ-системах, которые хранят и обрабатывают персональные данные.



## Стандарт ISO/IEC 29134:2017. Оценка воздействия на неприкосновенность частной жизни



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 29134:2017 «Информационные технологии - Методы и средства обеспечения безопасности – Оценка воздействия на неприкосновенность частной жизни – Руководство» (Information technology - Security techniques - Privacy impact assessment – Guidelines).

Стандарт определяет методику проведения «оценки воздействия на неприкосновенность частной жизни» (Data protection impact assessment – см. ст.35 GDPR) и устанавливает определенные рамки для такой оценки, с тем, чтобы уменьшить разноречивость в подходах и повысить качество. Стандарт позволит провести анализ воздействия предполагаемых в ходе обработки операций на защиту персональных данных, если такая обработка способна создать повышенные риски для прав и свобод физических лиц.

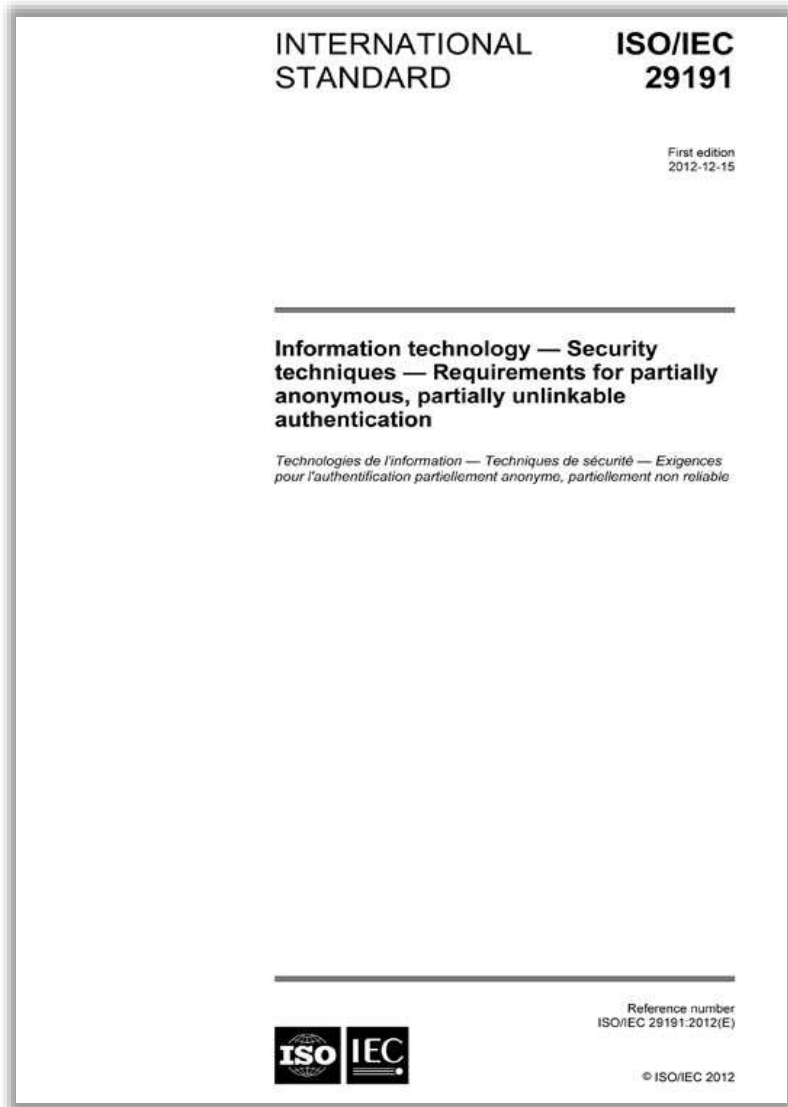
## Стандарт ISO/IEC 29151:2017. Свод практики по защите персональных данных



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 29151:2017 «Информационные технологии – Методы обеспечения безопасности – Свод практики по защите персональных данных» (Information technology - Security techniques - Code of practice for personally identifiable information protection).

Стандарт является непосредственным дополнением действующего стандарта ISO/IEC 27018:2014 «Информационные технологии - Методы обеспечения безопасности – Практика защиты персональных данных в публичных облаках, выступающих в роли обработчиков персональных данных» (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).

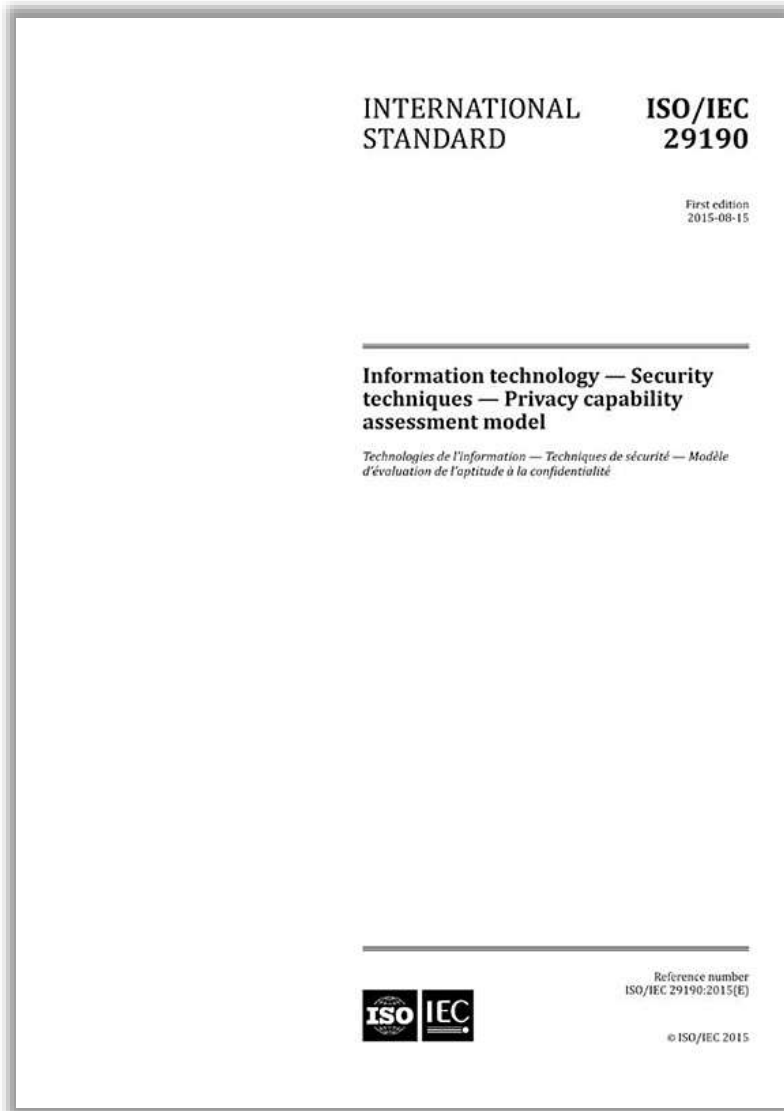
## Стандарт ISO/IEC 29191:2012. Требования к частично анонимной и частично несвязываемой аутентификации



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт 29191:2012 «Информационные технологии - Методы обеспечения защиты - Требования к частично анонимной и частично несцепляемой аутентификации» (Information technology - Security techniques - Requirements for partially anonymous, partially unlinkable authentication).

Текущий уровень техники для аутентификации пользователя требует раскрытия идентифицируемой информации аутентифицируемого пользователя. Во многих типах транзакций пользователь предпочел бы оставаться анонимным и не связываемым, что означает, что при выполнении двух транзакций трудно различить, выполняются ли транзакции одним и тем же пользователем или двумя разными пользователями. Тем не менее, в некоторых обстоятельствах существуют законные причины для возможности повторной идентификации (например, необходимость учета). Современные криптографические технологии предоставляют возможности реализации частично анонимной, частично несвязываемой аутентификации.

## Стандарт ISO/IEC 29190:2015. Оценка способности обеспечить неприкосновенность частной жизни



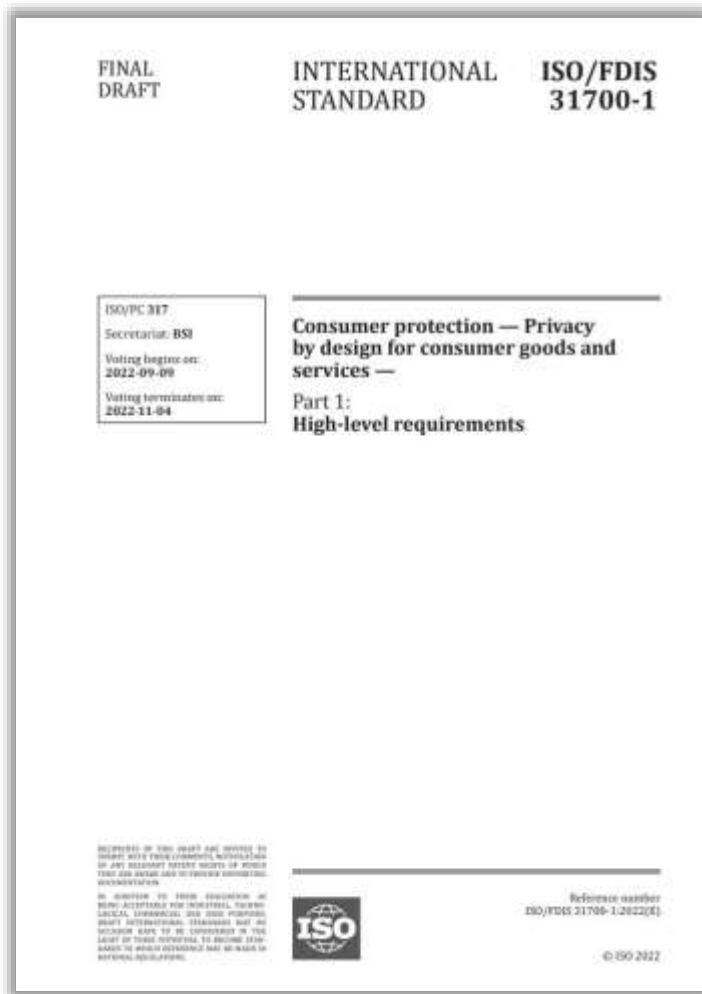
Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт 29190:2015 «Информационные технологии - Методы и средства обеспечения безопасности - Модель оценки способности обеспечить неприкосновенность частной жизни» (Information technology - Security techniques - Privacy capability assessment model).

Стандарт является высокоуровневым руководством для организаций по вопросам проведения ими оценки своих возможностей по управлению процессами, потенциально затрагивающими неприкосновенность частной жизни. В нём, в частности определены шаги, выполняемые в ходе оценки процессов на предмет их способности обеспечить защиту персональных данных, а также определен набор уровней способности обеспечить защиту персональных данных.



Международной организацией по стандартизации (International Organization for Standardization) был опубликован технический отчёт ISO/IEC TR 30110:2015 «Информационные технологии - Транс-юрисдикционные и социальные аспекты внедрения биометрических технологий - Биометрия и дети» (Information technology - Cross jurisdictional and societal aspects of implementation of biometric technologies - Biometrics and children).

## Проектируемая приватность для потребительских товаров и услуг



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт 31700-1:2023 «Защита прав потребителей – Проектируемая приватность для потребительских товаров и услуг – Часть 1: Высокоуровневые требования» (Consumer protection – Privacy by design for consumer goods and services – Part 1: High-level requirements) и технический отчёт ISO/TR 31700-2 «Защита прав потребителей – Проектируемая приватность для потребительских товаров и услуг – Часть 2: Варианты использования» (Consumer protection – Privacy by design for consumer goods and services – Part 2: Use cases).

Стандарт содержит общие рекомендации по разработке мер и возможностей, позволяющих потребителям обеспечивать соблюдение своих прав на неприкосновенность частной жизни; по назначению соответствующих ролей и полномочий; предоставлению потребителям соответствующей информации; проведению оценок рисков для неприкосновенности частной жизни; установлению и документированию требований к мерам и средствам обеспечения неприкосновенности частной жизни и способам их разработки; по управлению жизненным циклом персональных данных; а также по обеспечению готовности и реагированию в случае утечки данных.

## Европейский стандарт EN 17799:2023. Требования к защите персональных данных для операций по обработке данных

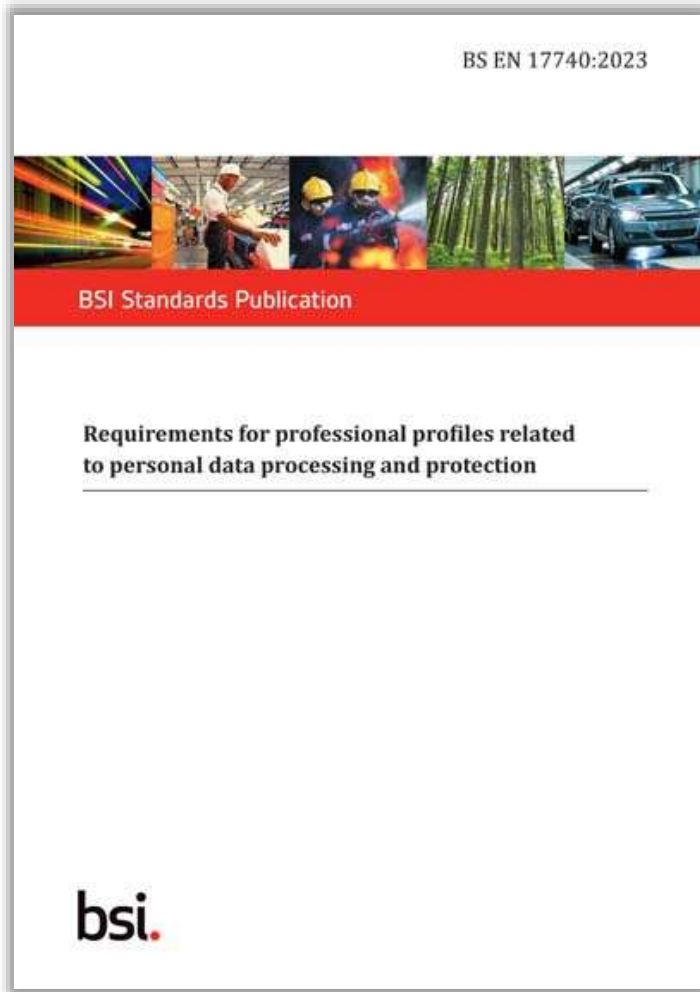


Европейский стандарт EN 17799:2023 «Требования к защите персональных данных для операций по обработке данных» (Personal data protection requirements for processing operations) устанавливает базовые требования к демонстрации соответствия деятельности по обработке персональных данных европейской нормативной базе по защите персональных данных, в соответствии со стандартом EN ISO/IEC 17065. Стандарт, однако не применяется в отношении продуктов или систем менеджмента, предназначенным для обработки персональных данных.

Документ применим в любых организациях, которые обрабатывают персональные данные в качестве операторов и/или обработчиков ПДн; и его цель заключается в том, чтобы предоставить набор требований, позволяющих таким организациям эффективно обеспечивать соответствие европейской нормативной базе по защите персональных данных.

Организация может принять решение о том, что стандарт применим только к определенному подмножеству её деятельности по обработке ПДн, если такое решение не влечёт за собой несоответствие европейской нормативной базе по защите персональных данных.

## Европейский стандарт BS EN 17740:2023. Требования к профессиональным профилям, связанным с обработкой и защитой персональных данных



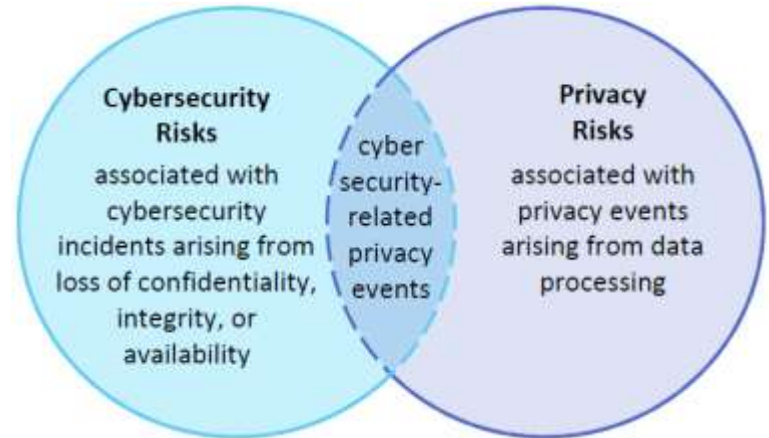
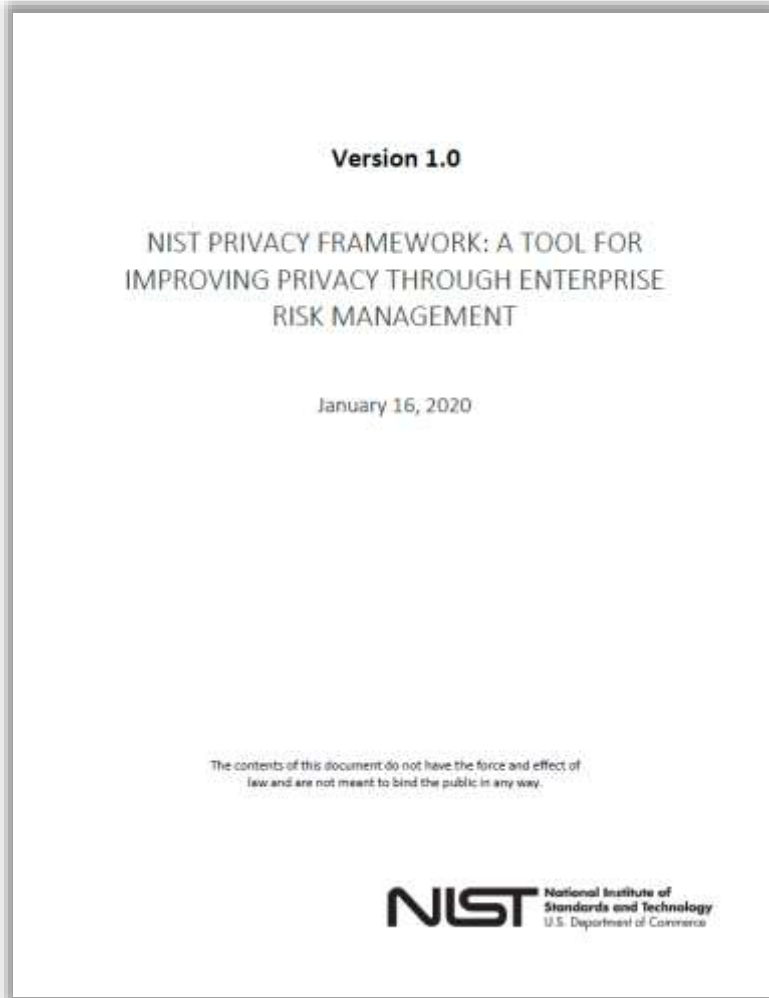
Британская версия европейского стандарта BS EN 17740:2023 «Требования к профессиональным профилям, связанным с обработкой и защитой персональных данных» (Requirements for professional profiles related to personal data processing and protection).

В документе установлены требования, связанные с профессиональной деятельностью лиц, занимающихся обработкой и защитой персональных данных, - а именно, интеллектуальной профессиональной деятельности, осуществляемой на разных уровнях сложности и в разных условиях деятельности (контекстах) как государственных, так и частных организаций.

Эти требования специфицируются, начиная с выявленных конкретных задач и видов деятельности, в терминах знаний, навыков и компетенций, в соответствии с Европейской системой квалификаций (European Qualifications Framework, EQF), - и представляются таким образом, чтобы, насколько это возможно, облегчить и способствовать гармонизации процессов оценки и валидации результатов обучения.



# NIST Privacy Framework: инструмент для обеспечения приватности через управление рисками в организации



## 690 Другие стандарты по защите персональных данных (1)

ISO/IEC 15944-8:2012 «Информационные технологии – Взгляд с точки зрения деловых операций. Часть 8. Выявление требований к защите персональных данных в качестве внешних ограничений на деловые операции» (Information technology - Business operational view - Part 8: Identification of privacy protection requirements as external constraints on business transactions)

<https://www.iso.org/standard/51544.html>

ISO/IEC 29187-1:2013 «Информационные технологии – Выявление требований к защите персональных данных, относящихся к обучению, образованию и тренировке (LET). Часть 1: Концепция и эталонная модель» (Information technology - Identification of privacy protection requirements pertaining to learning, education and training (LET) - Part 1: Framework and reference model)

<https://www.iso.org/standard/45266.html>

ISO 22307:2008 «Финансовые услуги – Оценка воздействия на неприкосновенность частной жизни» (Financial services - Privacy impact assessment) <https://www.iso.org/standard/40897.html>

ISO/TS 17975:2015 «Информатика в здравоохранении - Принципы и требования к данным для согласия на сбор, использование или раскрытие персональной информации о здоровье» (Health informatics - Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information) <https://www.iso.org/standard/61186.html>

ISO 22857:2013 «Информатика в здравоохранении – Руководство по защите персональных данных с целью содействия трансграничной передаче персональной информации о здоровье» (Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health data) <https://www.iso.org/standard/52955.html>

ISO/TS 14441:2013 «Информатика в здравоохранении – Требования по безопасности и защите персональных данных к системам управления электронными медицинскими документами, для использования при оценке соответствия» (Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment) <https://www.iso.org/standard/61347.html>

ISO 25237:2017 «Информатизация здоровья. Псевдонимизация» (Health informatics - Pseudonymization) <https://www.iso.org/standard/63553.html>

ISO/TR 12859:2009 «Интеллектуальные транспортные системы (ИТС) - Архитектура систем - Вопросы защиты неприкосновенности частной жизни в стандартах и системах ИТС» (Intelligent transport systems - System architecture - Privacy aspects in ITS standards and systems) <https://www.iso.org/standard/52052.html>

## 691 Другие стандарты по защите персональных данных (2)

ISO 16461:2018 «Интеллектуальные транспортные системы (ИТС) – Критерии защиты целостности и защиты персональных данных в системах бортовых транспортных датчиков» (Intelligent transport systems - Criteria for privacy and integrity protection in probe vehicle information systems) <https://www.iso.org/standard/56791.html>

ISO/TR 17427-7:2015 «Интеллектуальные транспортные системы (ITS) - Кооперативные ITS. Часть 7. Вопросы защиты неприкосновенности частной жизни» (Intelligent transport systems - Cooperative ITS - Part 7: Privacy aspects) <https://www.iso.org/standard/66959.html>

ISO/IEC TS 19608:2018 «Руководство по разработке функциональных требований к безопасности и защите персональных данных на основе ISO/IEC 15408» (Guidance for developing security and privacy functional requirements based on ISO/IEC 15408) <https://www.iso.org/standard/65459.html>

ISO/IEC 19086-4:2019 «Облачные вычисления - Концепция соглашений о качестве услуг (SLA) - Часть 4: Компоненты безопасности и защиты персональных данных» (Cloud computing - Service level agreement (SLA) framework - Part 4: Components of security and of protection of PII) <https://www.iso.org/standard/68242.html>

BS 10012:2017 «Защита персональных данных - Спецификации для системы менеджмента персональной информации» (Data protection. Specification for a personal information management system) <http://shop.bsigroup.com/ProductDetail/?pid=000000000030339453>

NIST SP 800-53 «Меры обеспечения безопасности и защиты персональных данных, рекомендуемые для федеральных информационных систем и организаций» (Security and Privacy Controls for Federal Information Systems and Organizations) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

NIST SP 800-144 «Руководство по обеспечению безопасности и защиты персональных данных при использовании публичных облачных вычислений» (Guidelines on Security and Privacy in Public Cloud Computing) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>

NIST SP 800-122 «Руководство по защите конфиденциальности персональных данных» (Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>

NIST SP 800-188 «Деидентификация государственных наборов данных» (De-Identifying Government Datasets) [http://csrc.nist.gov/publications/drafts/800-188/sp800\\_188\\_draft2.pdf](http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft2.pdf)

## Правоприменительная практика



Каждый член ЕС должен иметь один или несколько независимых государственных органов, которые будут нести ответственность за мониторинг применения GDPR - для защиты субъектов данных и содействия свободному потоку персональных данных в рамках Союза.

Надзорные органы публикуют ежегодный отчет о своей деятельности.

Надзорные органы должны сотрудничать друг с другом и с Европейской комиссией.

Если в государстве создано более одного надзорного органа, должен быть назначенный орган, который будет представлять эти органы в Европейском совете по защите данных (EDPB).

Европейский совет по защите данных:

- контролирует и обеспечивает правильное применение GDPR;
- консультирует Европейскую комиссию по любому вопросу, связанному с защитой данных в Союзе;
- предоставляет руководящие принципы, формат и процедуры для обмена информацией;
- издает руководящие принципы, рекомендации и лучшие практики для поощрения последовательного применения GDPR.

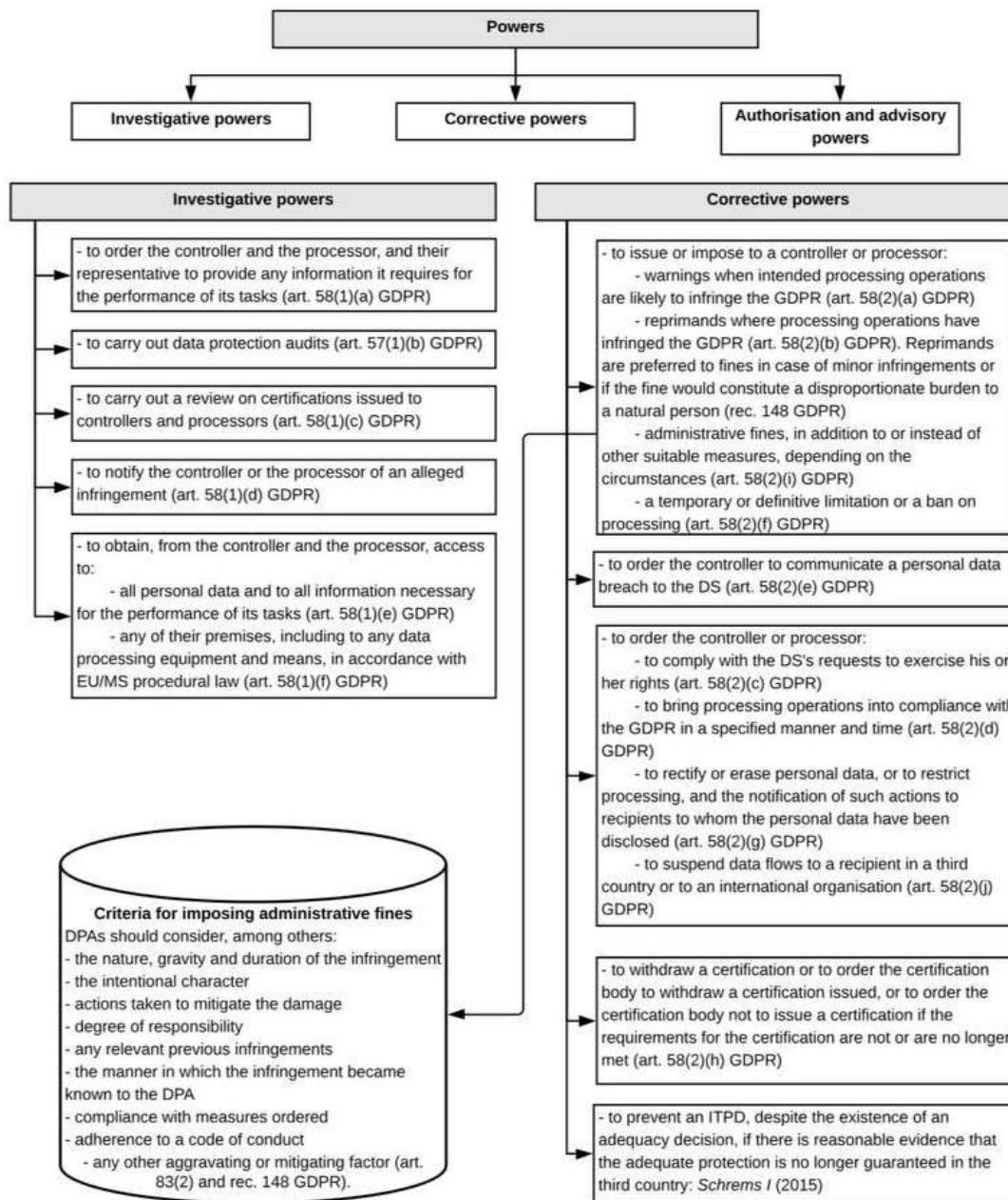
Надзорный орган при осуществлении своих задач и выполнении своих полномочий в соответствии с GDPR действует с полной независимостью.

Член или члены каждого надзорного органа должны, при выполнении своих задач и осуществлении своих полномочий:

- оставаться свободными от внешнего воздействия, будь то прямое или косвенное, а также не должны искать или получать указаний от кого бы то ни было;
- воздерживаться от любых действий, несовместимых с их обязанностями, а также не должны в течение срока их полномочий заниматься любым несовместимым видом деятельности, оплачиваемым или неоплачиваемым.

Каждому надзорному органу должны быть за государственный счет предоставлены кадровые, технические и финансовые ресурсы, помещения и инфраструктура, необходимые для эффективного выполнения его задач и осуществления его полномочий.

**Европейский совет по защите персональных данных** в ходе выполнения своих задач или осуществлении своих полномочий действует независимо и ни к кому не обращается за распоряжениями и не принимает их от кого бы то ни было.



## Разъяснения EDPS о существе и порядке проведения аудитов обработки персональных данных

### WHEN, WHY AND WHICH EUIS ARE AUDITED?

We carry out audits according to our Annual Inspection Plan. To establish this plan, we conduct a risk analysis and take into account the resources that are available for carrying out audits. Security audits of large scale IT systems and applications take place according to the laws governing their supervision.

Although we reserve the right to carry out audits on a random basis, we consider a variety of factors when deciding which EUI to audit, such as:

- the categories of data they process (e.g. health data are particularly sensitive);
- the number of complaints we receive about a particular EUI;
- whether the EUI regularly transfers data and to whom this data is transferred;
- compliance of the EUI with previous EDPS decisions;
- the EUI's overall history of cooperation with the EDPS.

With COVID-19 preventing the EDPS from conducting fieldwork, we adapted our audit planning and moved to remote audits by inspecting, for example, EUIs' public registers and their procedures when managing newsletter subscriptions. The format of remote audits is likely to be continued post-COVID-19 in a selection of circumstances.



### WHAT ARE THE 3 STAGES OF AN EDPS AUDIT?

1.

Before an EDPS inspection occurs, the EUI is usually informed at least four weeks in advance. At this stage, the EUI concerned or its Data Protection Officer (DPO) may be asked to provide information and documents to the EDPS.



During an on-the-spot audit, the EDPS meets the EUI's staff members responsible for the processing of personal data at their institution. The EDPS also requests information on and demonstrations of how the EUI processes individuals' personal data in its day-to-day work. The results of these meetings, interviews and demonstrations, as well as any evidence collected are recorded by the EDPS and are then submitted to the audited EUI for comments. Ensuring compliance means that we need to make sure that all recorded facts are correct. Consulting the EUI concerned is an opportunity for all actors involved in the audit to flag any misunderstandings about what has actually happened.

2.


3.

After an audit, the EDPS always provides appropriate feedback to the institution concerned in an audit report which contains a roadmap of recommendations to put in place where necessary. While the EDPS does not publish details of its audit reports, we regularly provide information on our audit activities in our Annual Reports and other publications. The EDPS always follows up on whether our recommendations included in the roadmap have been implemented.






## Комиссия ЕС предлагает новый процессуальный регламент для более эффективного применения GDPR в трансграничных случаях в ЕС



European Commission - Questions and answers



**Q&A: Stronger enforcement of the GDPR in cross-border cases**

Brussels, 4 July 2023

Today, the European Commission proposed new rules to support the effectiveness and efficiency of enforcement of the [General Data Protection Regulation \(GDPR\)](#) in cross-border cases. The [GDPR Procedural Regulation](#) aims to streamline cooperation between data protection authorities (DPAs), by harmonising some aspects of their administrative procedures in cross-border cases.

**Does this proposal change data protection rules?**

No. As we have seen, the GDPR works. The Commission's Procedural Regulation does not affect any substantial elements of the GDPR, such as the rights of data subjects, the obligations of data controllers and processors, or the lawful grounds for processing personal data as set by the GDPR.

In its [2020 report](#) on the application of the GDPR, the Commission found that procedural differences applied by DPAs hinder the smooth and effective functioning of the GDPR's cooperation and dispute resolution mechanisms in cross-border cases (i.e. when there are complainants located in more than one Member State).

The Commission identified that a more harmonised approach on issues such as complaint admissibility, the exercise of due process rights, and the involvement of complainants in the procedure would improve efficiency and results for citizens, businesses and data protection authorities alike. These elements were also identified as important by the European Parliament and the European Data Protection Board (EDPB).

**Does the proposal change the 'one-stop-shop' system?**

No. The regulation fully maintains and supports this system, where individuals and organisations can deal with their local/lead DPA. Individuals reap the benefits of the 'one-stop-shop' system every day, by relying on their local DPA to protect their rights, no matter where the organisation processing their data is based. Businesses also benefit from the right to deal with a single Data Protection Authority.

The proposal complements the GDPR by specifying detailed procedural rules for the cross-border enforcement system - the Regulation will operate within the framework established by the GDPR. It does not alter the procedural steps provided by the GDPR, nor the roles of the actors in the cross-border enforcement procedure - complainants, the lead DPA, DPAs concerned, or the EDPB.

**How do DPAs cooperate on cross-border cases?**

The GDPR is enforced by independent national DPAs, as well as national courts. In cases that involve cross-border processing of personal data (processing that takes place or substantially affects data subjects in more than one Member State) the GDPR's 'one-stop-shop' enforcement system applies. In such cases, the DPA where the entity under investigation is established conducts the investigation in cooperation with other relevant DPAs.

Under the GDPR, DPAs cooperate in order to reach consensus on the application of the GDPR. Where DPAs are unable to reach consensus in a cross-border case, the GDPR provides for dispute resolution by the European Data Protection Board (EDPB).

**How will DPAs cooperate under this proposal?**

The proposal introduces additional steps in the cooperation between DPAs to facilitate early consensus-building and to reduce disagreements later in the process which would require the use of the dispute resolution mechanism.

Early in an investigation, the lead DPA must send a 'summary of key issues' to their counter-parts concerned in the EU. This summary identifies the main elements subject to investigation and the lead DPA's views on the case. This will ensure that the DPAs concerned have all the necessary information to provide their views on the case at an early stage.

Европейская комиссия предложила 04.07.2023 проект нового регламента для поддержки эффективности и действенности применения GDPR путем упорядочения сотрудничества между органами по защите данных (DPA) и гармонизации некоторых аспектов их административных процедур в трансграничных случаях внутри ЕС. Предложенный регламент не затрагивает никаких существенных аспектов GDPR.

# Каталог решений сотрудничающих надзорных органов ЕС, принятых согласно ст.60 GDPR



HOME ABOUT EDPB NEWS OUR WORK & TOOLS

SEARCH

European Data Protection Board > Our Work & Tools > Consistency Findings > Register of Art. 60 Final Decisions

## Register of Art. 60 Final Decisions

LSA

CSA

Main legal reference

Keywords

Types of decision

APPLY FILTERS

RESET

ID	Date	LSA	CSA	Main legal reference	Keywords	Outcome	Summary document	Decision
EDPBI:FR:OSS D:2020:105	11/05/2020	FR SA	ES SA PT SA UK SA	<ul style="list-style-type: none"> <li>Article 17 (Right to erasure ('right to be forgotten'))</li> </ul>	<ul style="list-style-type: none"> <li>Data retention</li> <li>Right to erasure</li> </ul>	<ul style="list-style-type: none"> <li>Reprimand</li> </ul>	<a href="#">Summary</a>	<a href="#">Decision</a>
EDPBI:FR:OSS D:2020:89	25/02/2020	FR SA	BE SA DE BE SA DE HE SA DE MV SA DE NI SA DK SA ES SA FI SA SE SA UK SA	<ul style="list-style-type: none"> <li>Article 24 (Responsibility of the controller)</li> <li>Article 32 (Security of processing)</li> </ul>	<ul style="list-style-type: none"> <li>Data security</li> <li>Password</li> <li>Right of access</li> </ul>	<ul style="list-style-type: none"> <li>Reprimand</li> </ul>	<a href="#">Summary</a>	<a href="#">Decision</a>
EDPBI:FR:OSS D:2020:88	20/02/2020	FR SA	LU SA	<ul style="list-style-type: none"> <li>Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject)</li> <li>Article 21 (Right to object)</li> </ul>	<ul style="list-style-type: none"> <li>E-Commerce</li> <li>Right to object</li> </ul>	<ul style="list-style-type: none"> <li>Reprimand</li> </ul>	<a href="#">Summary</a>	<a href="#">Decision</a>
EDPBI:DEBE:OSS D:2020:87	19/02/2020	DE BE SA	AT SA BE SA ES SA FR SA IE SA PL SA PT SA UK SA	<ul style="list-style-type: none"> <li>Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject)</li> <li>Article 17 (Right to erasure ('right to be forgotten'))</li> </ul>	<ul style="list-style-type: none"> <li>Identity verification</li> <li>Right to erasure</li> <li>User account</li> </ul>	<ul style="list-style-type: none"> <li>Reprimand</li> </ul>	<a href="#">Summary</a>	<a href="#">Decision</a>



## Österreichische Datenschutzbehörde

Согласно [решению австрийского надзорного органа](#) из GDPR не вытекает право субъекта данных требовать реализации контролером какой-либо конкретной технической или организационной меры согласно требованиям ст.32 GDPR.



## **All public bins have been removed from the GPO due to potential privacy breaches under the General Data Protection Regulation (GDPR).**

Customers and visitors to the historic building will no longer be able to dispose their litter within the premises.

An Post says under the new privacy laws, even rubbish containing personal details is considered their responsibility.

For this reason, a decision was taken to remove every bin from the post office's main hall.

This was done on a trial basis.

A pensioner raised the issue on RTE's Liveline today to express her dismay over the new regulation.

"I was in the GPO last Saturday to send on a card and when I went to throw the cellophane away, I noticed that there was no bin under the counter," she said.

"So, I went to the next counter and to the big centre piece, but there were no bins anywhere.

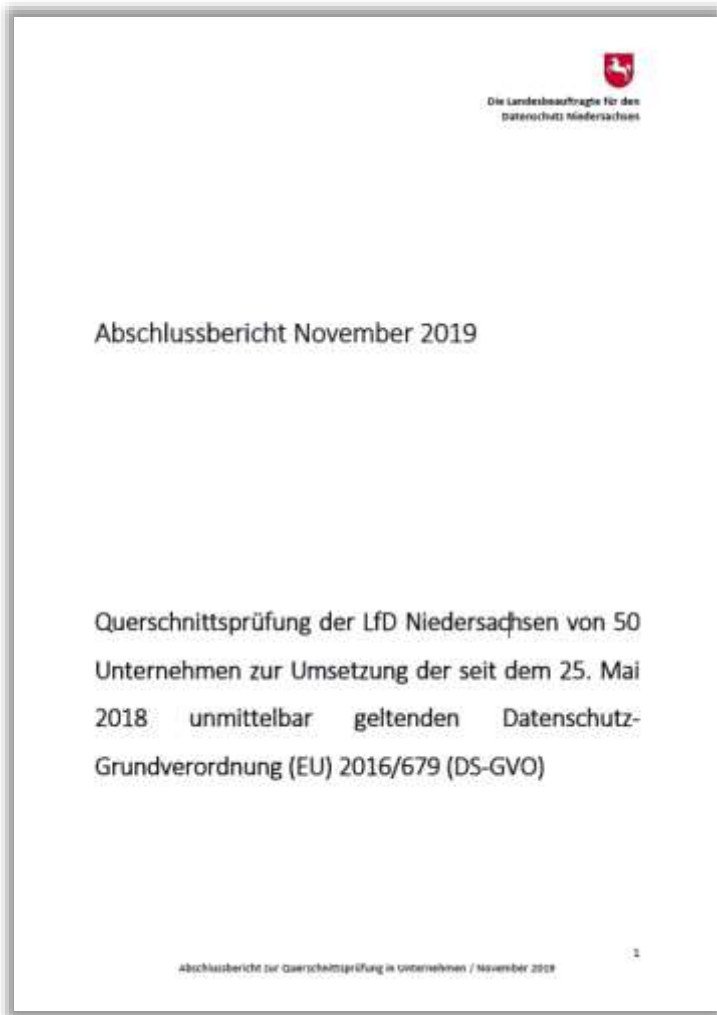
"I asked an [employee] who was going around with a big bag of rubbish asking what happened, and she said, 'we've removed them all because of the GDPR law'.

"I asked what relevance that has with litter bins and she said, 'I don't know, but we're crucified trying to keep the place clean. You have to leave your rubbish on the counter or else throw it on the floor'."

Установка в отделениях почты мусорных корзин находится вне регулирования GDPR, т.к. не является обработкой персональных данных, указанной в ст.2 GDPR, поскольку выбрасываемые в урны бумаги с личной информацией не образуют систему данных (filing system).

Правда, оценка рисков DPIA могла показать, что необходимы информационные объявления, закрывающиеся урны и шредеры, но это уже другое дело.

## Комиссар по защите данных Нижней Саксонии опубликовал сводный отчет по проверке 50 компаний



Государственный Комиссар по защите данных земли Нижняя Саксония (Die Landesbeauftragte für den Datenschutz Niedersachsen) опубликовал сводный отчет по проверке 50 компаний на соответствие GDPR, из которых продемонстрировали: удовлетворительный уровень – 9, неудовлетворительный уровень – 32, плохой уровень – 8. Некоторые выявленные недостатки:

- неприменение концептов Data protection by design and by default;
- не учитывались требования по проведению обязательного DPIA, не документировались решения об отсутствии необходимости проведения DPIA, недостаточное описание процессов обработки данных, недостаточный объем мер по снижению рисков;
- явно не определена процедура обновления RoPA, не все процессы учтены в RoPA (сбор данных на веб-сайте, работа с кандидатами), в RoPA не указана контактная информация;
- использование согласия при наличии других правовых оснований, не использование гранулированных согласий, не указание сведений о порядке и возможности отзыва согласия;
- использование шаблонных политик без адаптации под процессы компании, недостаточное описание баланса интересов (при выборе законного интереса как правового основания для обработки данных), неэффективные процессы проверки личности субъектов и предоставления копий данных по запросу;
- DPO проводил DPIA без формального подтверждения своих компетенций.

## CNIL осуществляет автоматизированный надзор по соблюдению сайтами требований в отношении cookies

**CNIL.**

*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

MES DÉMARCHES | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL   

Refuser les cookies doit être aussi simple qu'accepter : mise en conformité de tous les organismes mis en demeure et actions à venir de la

### Refuser les cookies doit être aussi simple qu'accepter : mise en conformité de tous les organismes mis en demeure et actions à venir de la CNIL

29 juin 2021

*Un mois après leur mise en demeure, la vingtaine d'organismes qui ne permettaient pas aux internautes de refuser les cookies aussi facilement que de les accepter se sont tous mis en conformité. La Présidente de la CNIL ayant décidé de poursuivre la campagne de vérifications, de nouvelles mesures correctrices seront prises à l'encontre d'autres organismes qui ne seraient pas en conformité sur ce point.*

Le 18 mai 2021, la Présidente de la CNIL a décidé de mettre en demeure une vingtaine d'organismes éditant des sites à forte fréquentation et ayant des pratiques contraires à la législation sur les cookies. Cette action s'inscrit dans le cadre de la stratégie globale de mise en conformité initiée par la CNIL depuis 2 ans et qui s'est concrétisée, le 1<sup>er</sup> octobre 2020, par l'adoption des lignes directrices et d'une recommandation. Les acteurs concernés avaient alors été invités à s'assurer de la conformité de leurs pratiques à ces nouvelles règles, dans un délai de six mois, soit au plus tard fin mars 2021.

Tous les organismes visés par ces mises en demeure, y compris d'importantes sociétés de l'économie numérique, se sont mis en conformité et ont modifié leurs pratiques afin de permettre aux internautes de refuser les cookies aussi facilement que de les accepter.

Cette première campagne de vérifications et de mesures correctrices sera suivie d'actions similaires au cours des prochains mois. Elle témoigne de l'engagement ferme de la CNIL d'obtenir une conformité globale des acteurs s'adressant aux internautes français et ainsi à faire respecter leur vie privée.

D'autres acteurs éditant des sites web à forte fréquentation ne sont pas encore en conformité. D'autres mises en demeure pourraient être prononcées et plusieurs procédures de sanction ont déjà été lancées. Pour rappel, en cas de non-conformité à la législation sur les cookies, les organismes encourent des sanctions pécuniaires pouvant aller jusqu'à 2 % de leur chiffre d'affaires.

Национальная комиссия по информатике и свободе Франция (CNIL) проводит автоматизированные проверки практик сайтов на предмет хранения файлов cookie. Уже было проверена 1,000 веб-сайтов с наибольшим трафиком во Франции, и некоторые из них были подвергнуты административным санкциям.

CNIL объявила 29.06.2021 о продолжении программы в отношении менее популярных сайтов.

# 5 MOST COMMON GDPR MISTAKES

That large companies make and  
how can you avoid these?

Punit BHATIA

1. **A project approach** - подход к GDPR-комплаенсу, как к разовому проекту. Решение: планировать и проводить регулярные мероприятия.
2. **Not measuring** - не измерять эффективность внедрённых контролей. Решение: вводить и отслеживать метрики (KPI).
3. **Relying on consent** - отдавать преимущество согласию как правовому основанию для обработки данных. Решение: выбирать согласие только в крайнем случае.
4. **Focus on IT data** - забывать про данные на бумажных носителях, к примеру, и связанных с этим процессах. Решение: инвентаризация всех информационных активов.
5. **Third party audits** - ограничиваться только договорами, не проверяя самих поставщиков и партнеров. Решение: Supplier Security Management.

## Сборник прецедентов в отношении реализации прав на возражение и забвение



В документе рассматривается подборка решений по принципу "одного окна", взятых из публичного реестра EDPB и относящихся к статьям 17 и 21 GDPR. Большинство жалоб касаются незначительных нарушений и часто характеризуются оперативным устранением нарушения с о стороны контролера. Таким образом, выговоры/предупреждения от надзорных органов являются основным результатом рассмотренных решений.

В тех случаях, когда компетентный надзорный орган налагал конкретные санкции на контролеров данных, это обычно было связано с большим количеством нарушений GDPR, при этом незначительную роль играли нарушения статей 17 и 21.

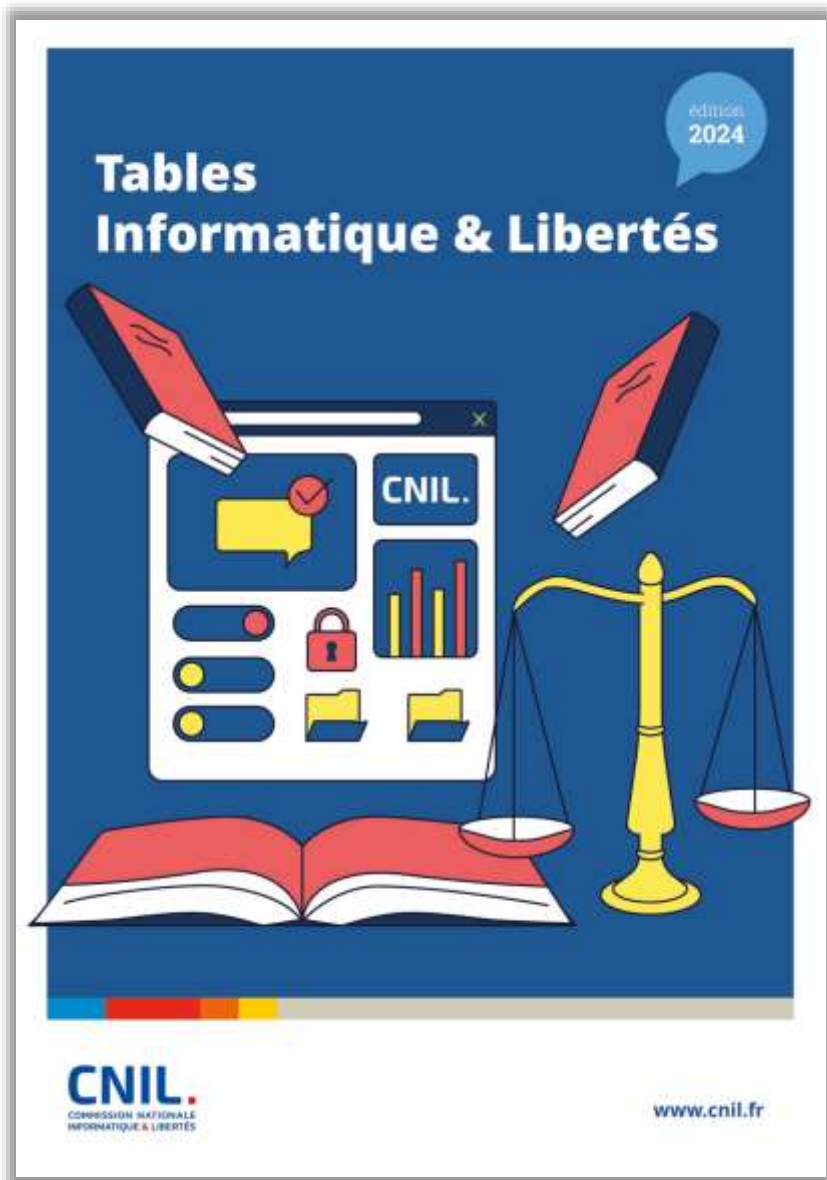




DPC выпустила брошюру, содержащую 126 примеров из практики DPC за первые пять лет действия GDPR. Эти примеры разбиты по категориям и проиндексированы, что облегчает поиск соответствующих примеров и является ценным справочным пособием при изучении того, как DPC рассматривает жалобы.

Примеры разбиты на следующие категории:

- Жалобы на непредоставление доступа к данным
- Точность данных
- Трансграничные жалобы
- Уведомление об утечке данных
- (Несанкционированное) раскрытие данных
- Электронный прямой маркетинг
- Уничтожение данных
- Директива о правоприменении (LED)
- Возражение против обработки данных
- Ограничение цели обработки данных
- Прозрачность обработки данных



Французский CNIL в декабре 2023г. опубликовал сборник правоприменительной практики, в котором собраны и систематизированы резюме многочисленных решений французских и европейских судов, в частности Европейского суда по правам человека, Суда Европейского союза, Конституционного совета, Государственного совета и Кассационного суда. В него также включены некоторые решения Европейского комитета по защите данных (EDPS) и самого CNIL, причем особое внимание уделяется тем из них, которые устанавливают новую доктрину или определяют принципы обработки и защиты персональных данных.

[https://www.cnil.fr/sites/cnil/files/2023-12/tables\\_informatique\\_et\\_libertes.pdf](https://www.cnil.fr/sites/cnil/files/2023-12/tables_informatique_et_libertes.pdf)

<https://www.cnil.fr/fr/tables-informatique-et-libertes-la-cnil-publie-sa-doctrine-en-matiere-de-protection-des-donnees>

## Надзорный орган не может свободно выбирать, какие дела расследовать, а какие нет

The screenshot shows the Norwegian Data Protection Authority (DPA) website. The main heading is "PVN-2023-14 Klage over Datatilsynets avgjørelse om å avslutte sak uten å ta stilling til om personopplysningsloven er brutt". Below the heading, it states the release date: "Datatilsynets uttalelse: 21/01/2023". The case involves a complaint from Mari Bø Haugstad, Bjørnar Borvik, Hans Marius Graasvold, Ellen Økland Blinkenberg, Hans Marius Tessem, and Morten Goodwin, Malin Tønseth, filed on 7 November 2023. The summary describes the complaint regarding the DPA's decision to close a case without a ruling on whether the Personal Data Act was violated. It details the timeline from the initial complaint in March 2021 to the final decision in January 2023, including the DPA's reasoning and the complainants' appeals.

Субъект данных подал жалобу в норвежский DPA, который решил просто проинформировать контролера о его обязательствах по GDPR и закрыл дело без дальнейшего расследования. Не удовлетворившись этим, субъект данных оспорил решение о закрытии дела. После некоторого обмена мнениями DPA пересмотрел свое решение, но в итоге оставил его в силе. В соответствии с национальными процедурами дело было передано в Апелляционный совет по защите персональных данных. Перед ним была поставлена задача определить, может ли DPA закрыть дело, просто направив контролеру информационное письмо без оценки каких-либо нарушений GDPR, или же субъект данных может потребовать от DPA рассмотреть его дело и вынести решение о законности обработки его персональных данных.

Норвежский апелляционный совет по защите частной жизни отменил решение DPA о закрытии дела по жалобе только информационным письмом в адрес контролера, обязав его оценить законность обработки, подчеркнув, что DPA не может свободно выбирать, какие дела расследовать, а какие нет. В качестве основания для этого было использовано право субъекта персональных данных на подачу жалобы в соответствии со статьей 77 GDPR в сочетании со статьей 141 и статьей 57(1)(f) GDPR.

## Штрафы - базы дел и аналитика



## ст.82 GDPR

1. Любое лицо, которое понесло материальный или нематериальный ущерб в результате нарушения положений настоящего Регламента, имеет право на получение компенсации от контролёра или процессора за понесенный ущерб.
2. Любой контролёр, участвующий в обработке, несет ответственность за ущерб, причиненный в результате обработки, нарушающей GDPR. Процессор несет ответственность за ущерб, причиненный в результате обработки только если он не выполнил требования GDPR, специально установленные для процессоров, или если он действовал за рамками или в нарушение законных распоряжений контролёра.
3. Контролёр или процессор освобождается от ответственности, упомянутой в параграфе 2, если докажет, что никоим образом не несет ответственность за событие, которое явилось причиной ущерба.

**Ст.83 GDPR** – каждый надзорный орган может наложить административные санкции (в зависимости от того, что выше):

- До € 10 000 000 или 2% годового оборота - например, за нарушение правила “privacy by design”
- До € 20 000 000 или 4% годового оборота - например, за нарушение принципов защиты данных или обработку данных без согласия субъекта данных

**Ст.84 GDPR** – Государства (участники ЕЭЗ) устанавливают нормы относительно иных санкций, применимых за нарушения GDPR, в том числе за нарушения, которые не подпадают под административные штрафы, а также принимают все меры, для того, чтобы обеспечить их применение. Такие санкции должны быть эффективными, соизмеримыми и должны оказывать сдерживающее воздействие.

**Статья 226-20 Уголовного кодекса Французской Республики:**






Хранение персональных данных сверх срока, предусмотренного законом или постановлением, заявлением о разрешении или заключении, или предварительным заявлением, направленным в Национальную комиссию по информационным технологиям и свободам (CNIL), наказывается тюремным заключением сроком на пять лет и штрафом в 300,000 евро, если такое хранение не ведется для исторических, статистических или научных целей в соответствии с условиями, изложенными в законе.

**GDPR Enforcement Tracker** backed by **CMS**  
LAW FIRM

This website contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any indication of further GDPR fines and penalties.

**The Netherlands: First GDPR fine** **UK: 204.6 Mio fine proposed** **Germany: FI**  
 First GDPR fine from the Netherlands over 400k EUR. [Link](#) The ICO issued a notice of its intention to fine British Airways GBP 183.38 Mio for GDPR infringements (no final decision) [Link](#) First fine ago

Show  entries Search:

Country	Authority	Date	Fine	Controller/Processor	Quoted Article	Summary	Info
 UNITED KINGDOM	Information Commissioner (ICO)	2018-07-06	204,600,000	British Airways	Art. 32 GDPR	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other member states have made their representations. The ICO issued a notice of its intention to fine British Airways £183.38M for GDPR infringements which likely involve a breach of Art. 32 GDPR. The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018. The ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well as name and address information.	<a href="#">Link</a>
 UNITED KINGDOM	Information Commissioner (ICO)	2019-07-09	110,390,200	Marriott International, Inc	Art. 32 GDPR	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other member states have made their representations. The ICO issued a notice of its intention to fine Marriott International Inc which relates to a cyber incident which was notified to the ICO by Marriott in November 2018. GDPR infringements are likely to involve a breach of Art. 32 GDPR. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 21 countries in the European Economic Area (EEA). Seven million related to UK residents. It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.	<a href="#">Link</a>
 FRANCE	French Data Protection Authority (CNIL)	2019-01-21	50,000,000	Google Inc.	Art. 15 GDPR, Art. 14 GDPR, Art. 8 GDPR, Art. 4 nr. 11 GDPR, Art. 5 GDPR	The fine was imposed on the basis of complaints from the Austrian organisation "None Of Your Business" and the French NGO "La Quadrature du Net". The complaints were filed on 29th and 29th of May 2018 - immediately after the DSGVO became applicable. The complaints concerned the creation of a Google account during the configuration of a mobile phone using the Android operating system. The CNIL imposed a fine of 50 million euros for lack of transparency (Art. 5 GDPR), insufficient information (Art. 13 / 14 GDPR) and lack of legal basis (Art. 6 GDPR). The obtained consents had not been given "specific" and not "unambiguous" (Art. 4 nr. 11 GDPR).	<a href="#">Link</a>
 BULGARIA	Data Protection Commission of Bulgaria (KZLD)	2019-08-26	2,500,000	National Revenue Agency	Art. 31 GDPR	Leakage of personal data in a hacking attack due to inadequate technical and organisational measures to ensure the protection of information security. It was found that personal data concerning about 6 million persons was illegally accessible.	<a href="#">Link</a>
 BULGARIA	Data Protection Commission of Bulgaria (KZLD)	2019-08-28	511,000	DSK Bank	Art. 32 GDPR	Leakage of personal data due to inadequate technical and organisational measures to ensure the protection of information security. Third parties had access to over 28000 credit records relating to over 33000 bank customers including personal data such as names, citizenships, identification numbers, addresses, copies of identity cards and biometric data.	<a href="#">Link</a>

## GDPR Enforcement Tracker

Общедоступная онлайн-база сведений об известных случаях привлечения к юридической ответственности за нарушение GDPR. База регулярно актуализируется.

The screenshot displays the IAPP FTC Casebook interface. At the top, the IAPP logo is on the left, and navigation links for News, Contact, Train, Certify, Resources, Conferences, and Join are in the center. A STORE button is on the right. Below the navigation is a large banner image of a classical building facade with the text "FTC Casebook" and sub-links for "Unrollme Inc. v. FTC", "Consent", and "Actions".

Below the banner is a search bar and a "Filter By:" section with various categories: Start Date, End Date, Subject, FPP, Industry, Industry Practices, Legal Issues, Remedies, Section 5, Security, and Statutory. The main content area shows a list of cases, all dated August 8, 2019, involving Unrollme Inc. Each entry includes a title, a link to the full case, and a brief summary.

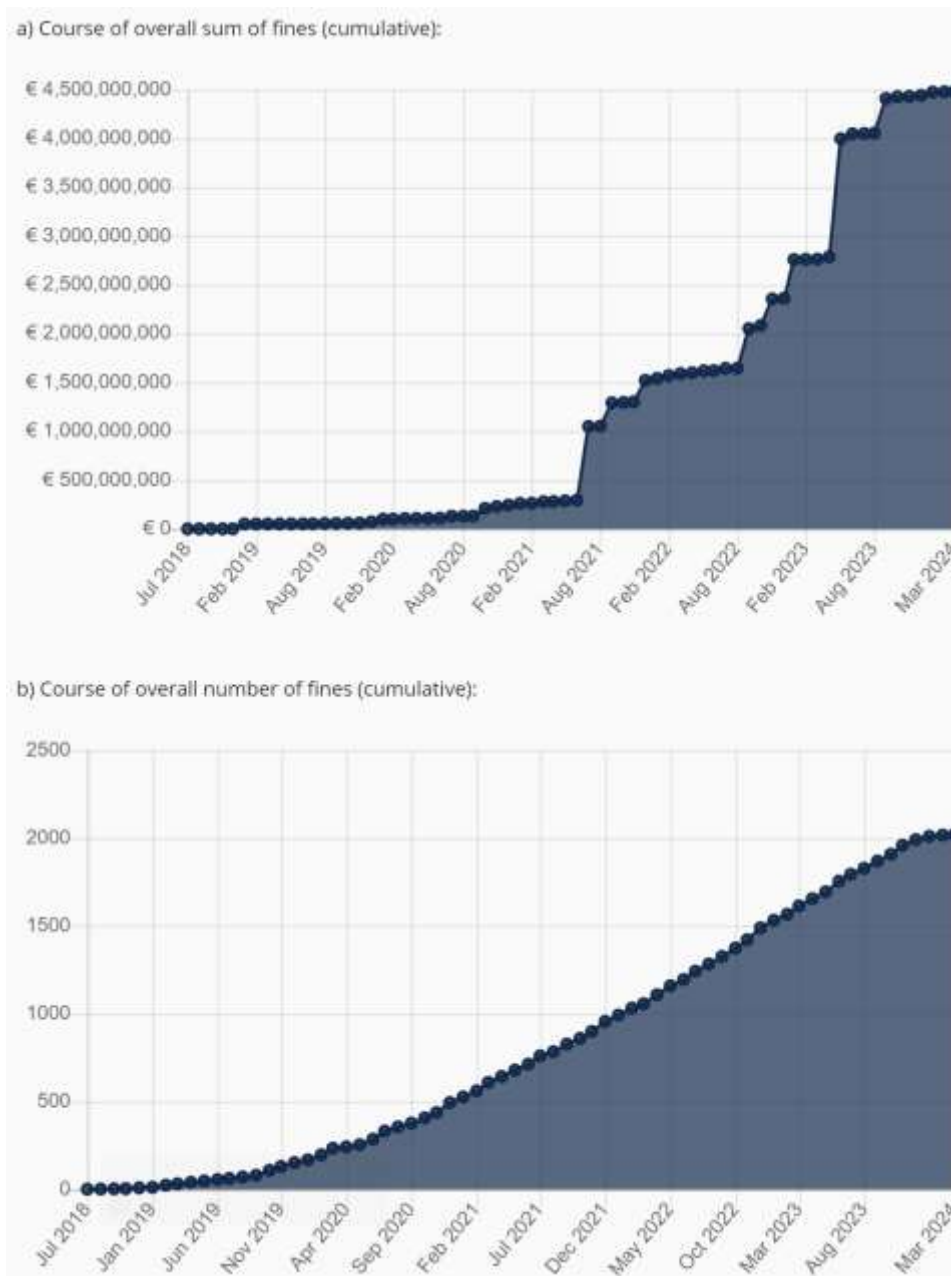
Date	Case Title	Summary
Aug 8, 2019	<b>Unrollme Inc. -- Agreement Containing Consent Order</b>	UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION in the Matter of UNROLLME INC., a corporation, FILE NO. 172 3139 AGREEMENT CONTAINING CONSENT ORDER
Aug 8, 2019	<b>Unrollme Inc. -- Analysis to Aid Public Comment</b>	Analysis of Proposed Consent Order to Aid Public Comment in the Matter of Unrollme Inc., File No. 1723139 The Federal Trade Commission ("Commission") has accepted
Aug 8, 2019	<b>Unrollme Inc. -- Complaint</b>	UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION COMMISSIONERS: Joseph J. Simons, Chairman Noah Joshua Phillips Rohit Chopra Rebecca Kelly Slaughter Christine S. Wilton
Aug 8, 2019	<b>Unrollme Inc. -- Separate Statement of Commissioner Noah Joshua Phillips</b>	Separate Statement of Commissioner Noah Joshua Phillips Federal Trade Commission v. Unrollme Inc. Matter No. 1723139 August 8, 2019 I join my colleagues in supporting
Aug 8, 2019	<b>Unrollme Inc.</b>	An email management company will be required to delete personal information it collected from consumers as part of a settlement with the Federal Trade Commission

## International Association of Privacy Professionals

Общедоступная онлайн-база сведений об известных случаях привлечения к юридической ответственности за нарушение требований Privacy and Data Security. База регулярно актуализируется.

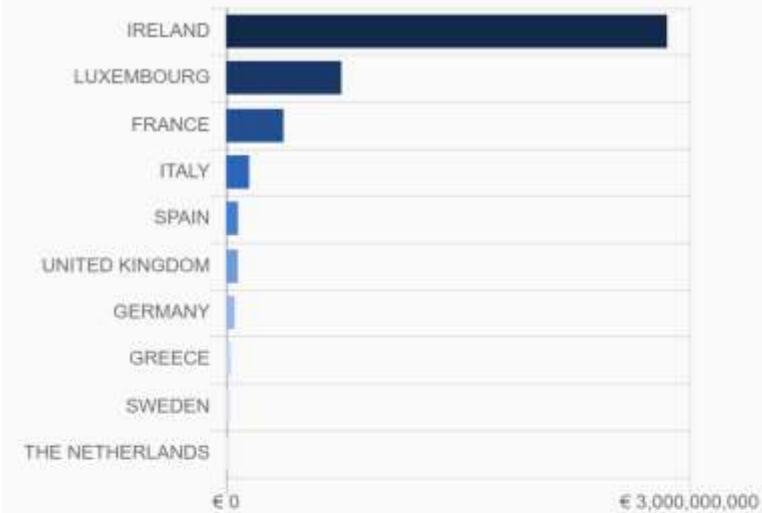


## 713 Объем и количество наложенных штрафов – общая статистика



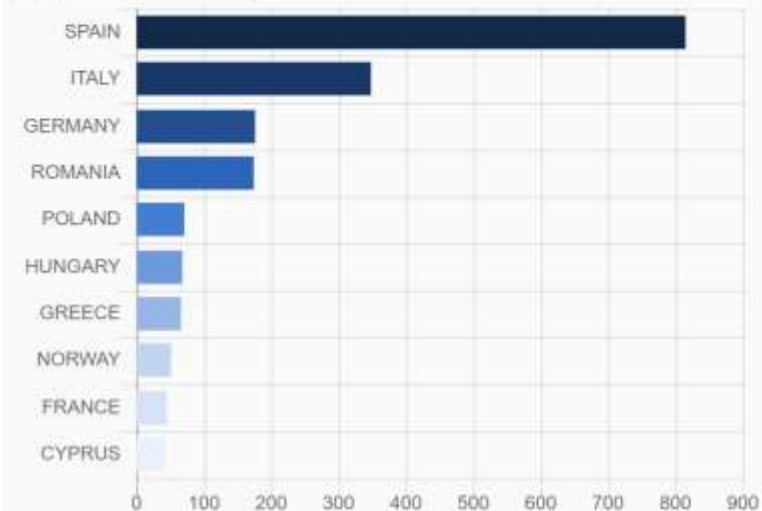
## 714 Статистика наложенных штрафов по Топ-10 стран

1. By total sum of fines:



Country	Sum of Fines
IRELAND	€ 2,855,363,400 (at 27 fines)
LUXEMBOURG	€ 746,314,000 (at 32 fines)
FRANCE	€ 371,699,300 (at 45 fines)
ITALY	€ 149,314,327 (at 348 fines)
SPAIN	€ 77,224,030 (at 815 fines)
UNITED KINGDOM	€ 75,532,800 (at 14 fines)
GERMANY	€ 55,388,233 (at 176 fines)
GREECE	€ 31,077,000 (at 66 fines)
SWEDEN	€ 26,462,230 (at 38 fines)
THE NETHERLANDS	€ 24,924,500 (at 24 fines)

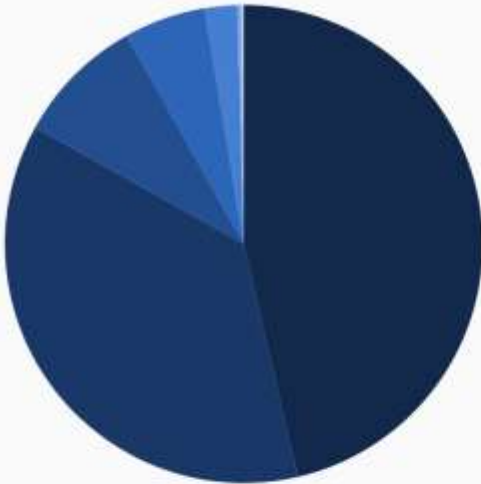
2. By total number of fines:



Country	Number of Fines
SPAIN	815 (with total € 77,224,030)
ITALY	348 (with total € 149,314,327)
GERMANY	176 (with total € 55,388,233)
ROMANIA	174 (with total € 1,116,950)
POLAND	71 (with total € 3,600,269)
HUNGARY	68 (with total € 2,518,861)
GREECE	66 (with total € 31,077,000)
NORWAY	51 (with total € 12,117,950)
FRANCE	45 (with total € 371,699,300)
CYPRUS	42 (with total € 1,429,000)

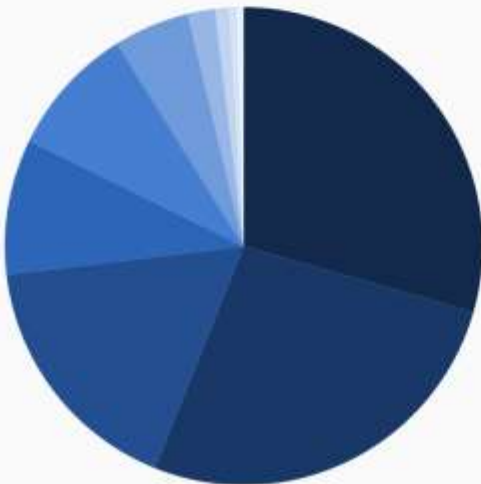
## Объем и количество наложенных штрафов в зависимости от причины нарушения

### 1. By total sum of fines:



Violation	Sum of Fines
Non-compliance with general data processing principles	€ 2,081,076,159 (at 566 fines)
Insufficient legal basis for data processing	€ 1,649,632,012 (at 626 fines)
Insufficient technical and organisational measures to ensure information security	€ 391,263,875 (at 362 fines)
Insufficient fulfilment of information obligations	€ 247,483,060 (at 188 fines)
Insufficient fulfilment of data subjects rights	€ 98,376,170 (at 195 fines)
Unknown	€ 9,300,700 (at 10 fines)
Insufficient cooperation with supervisory authority	€ 6,211,029 (at 109 fines)
Insufficient fulfilment of data breach notification obligations	€ 2,675,582 (at 39 fines)
Insufficient data processing agreement	€ 1,057,110 (at 11 fines)
Insufficient involvement of data protection officer	€ 955,300 (at 20 fines)

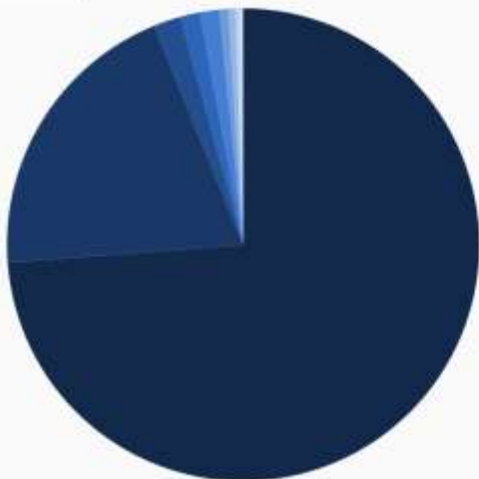
### 2. By total number of fines:



Violation	Number of Fines
Insufficient legal basis for data processing	626 (with total € 1,649,632,012)
Non-compliance with general data processing principles	566 (with total € 2,081,076,159)
Insufficient technical and organisational measures to ensure information security	362 (with total € 391,263,875)
Insufficient fulfilment of data subjects rights	195 (with total € 98,376,170)
Insufficient fulfilment of information obligations	188 (with total € 247,483,060)
Insufficient cooperation with supervisory authority	109 (with total € 6,211,029)
Insufficient fulfilment of data breach notification obligations	39 (with total € 2,675,582)
Insufficient involvement of data protection officer	20 (with total € 955,300)
Insufficient data processing agreement	11 (with total € 1,057,110)
Unknown	10 (with total € 9,300,700)

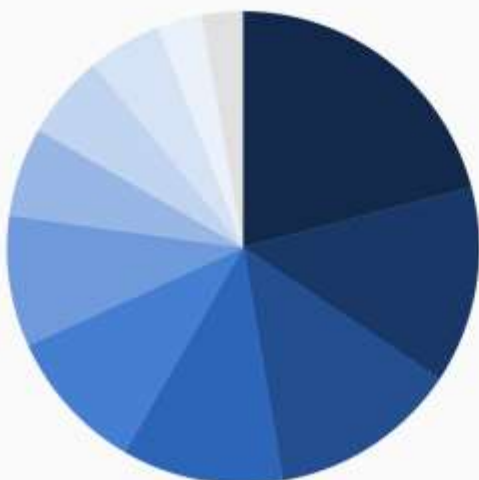
## Объем и количество наложенных штрафов в зависимости от отрасли/сектора деятельности

1. By total sum of fines;



Sector	Sum of Fines
Media, Telecoms and Broadcasting	€ 3,312,607,366 (at 287 fines)
Industry and Commerce	€ 898,655,601 (at 444 fines)
Transportation and Energy	€ 84,504,570 (at 107 fines)
Finance, Insurance and Consulting	€ 60,155,158 (at 209 fines)
Employment	€ 59,026,077 (at 130 fines)
Public Sector and Education	€ 27,571,063 (at 235 fines)
Accomodation and Hospitality	€ 22,490,048 (at 65 fines)
Health Care	€ 16,796,709 (at 191 fines)
Real Estate	€ 2,601,831 (at 60 fines)
Individuals and Private Associations	€ 1,857,366 (at 275 fines)
Not assigned	€ 1,765,208 (at 123 fines)

2. By total number of fines;

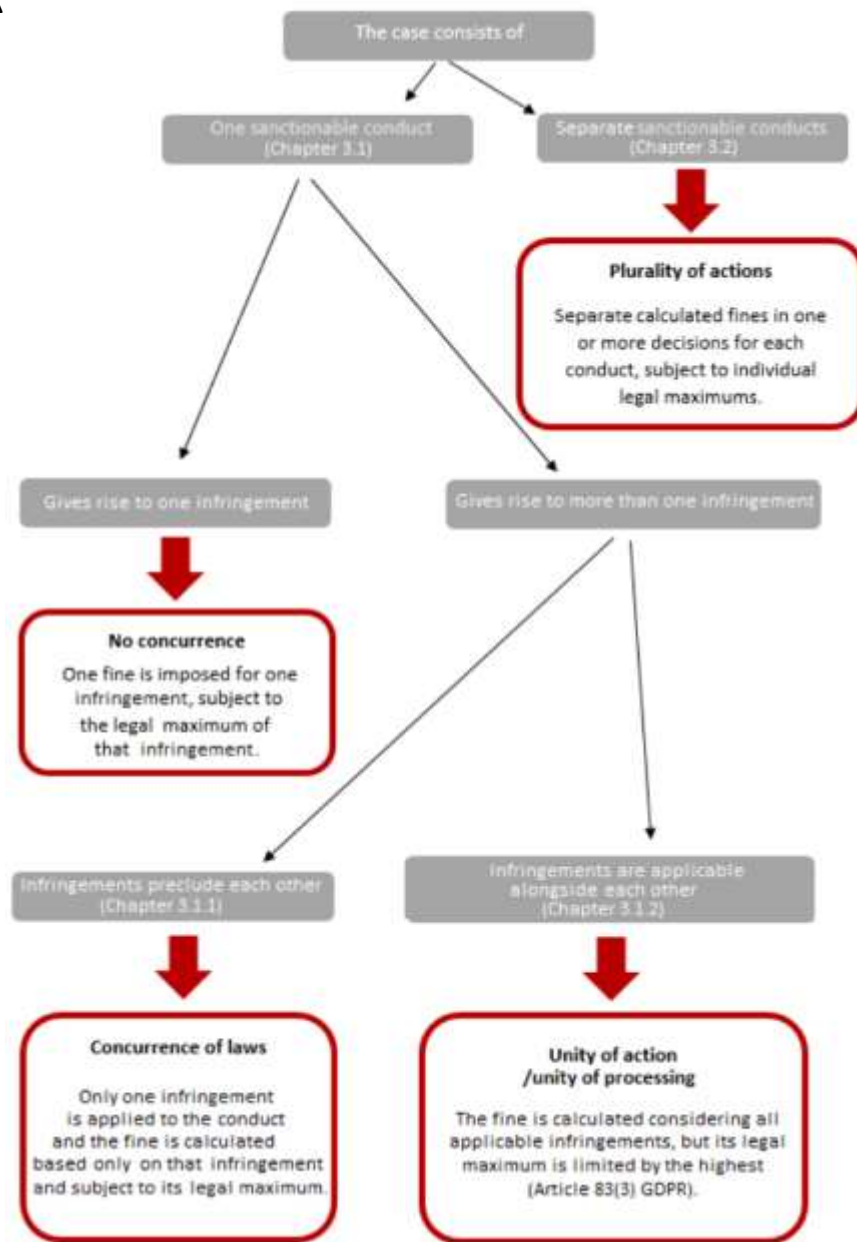
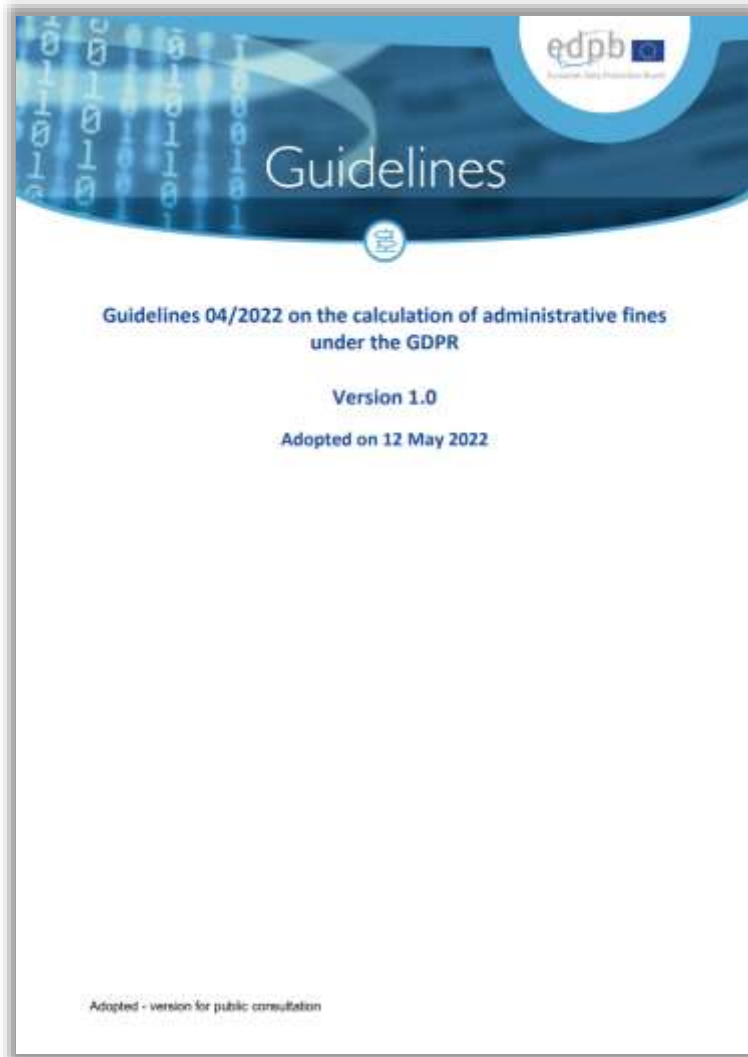


Sector	Number of Fines
Industry and Commerce	444 (with total € 898,655,601)
Media, Telecoms and Broadcasting	287 (with total € 3,312,607,366)
Individuals and Private Associations	275 (with total € 1,857,366)
Public Sector and Education	235 (with total € 27,571,063)
Finance, Insurance and Consulting	209 (with total € 60,155,158)
Health Care	191 (with total € 16,796,709)
Employment	130 (with total € 59,026,077)
Not assigned	123 (with total € 1,765,208)
Transportation and Energy	107 (with total € 84,504,570)
Accomodation and Hospitality	65 (with total € 22,490,048)
Real Estate	60 (with total € 2,601,831)


## 717 **Топ-10 самых больших штрафов за 2018-2023гг.**

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	1200000000	Insufficient legal basis for data processing	2023-05-12
2	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746000000	Non-compliance with general data processing principles	2021-07-16
3	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405000000	Non-compliance with general data processing principles	2022-09-05
4	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	390000000	Non-compliance with general data processing principles	2023-01-04
5	TikTok Limited	Media, Telecoms and Broadcasting	IRELAND	345000000	Non-compliance with general data processing principles	2023-09-01
6	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	265000000	Insufficient technical and organisational measures to ensure information security	2022-11-25
7	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225000000	Insufficient fulfilment of information obligations	2021-09-02
8	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90000000	Insufficient legal basis for data processing	2021-12-31
9	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60000000	Insufficient legal basis for data processing	2021-12-31
10	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60000000	Insufficient legal basis for data processing	2021-12-31

## Руководство EDPB о методике расчета административных штрафов за неисполнение норм GDPR



# Методика по расчету и наложению штрафов в Нидерландах (2019.05)



## STAATSCOURANT

Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.

Nr. 14586  
14 maart  
2019

---

**Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019)**

De Autoriteit Persoonsgegevens heeft, geleid op de artikelen 4:81 en 5:46, tweede lid, van de Algemene wet bestuursrecht, artikel 83 van de Algemene verordening gegevensbescherming, artikelen 14, derde lid, 17 en 18 van de Uitvoeringswet Algemene verordening gegevensbescherming, artikel 2:11a van de Kieswet, artikel 4:1, eerste lid, van de Wet basisregistratie personen, artikel 35c van de Wet politiegegevens, artikelen 27, 39; 51, 51d en 51h van de Wet justitiële en strafvorderlijke gegevens en artikel 15:4, vierde en vijfde lid, van de Telecommunicatiewet, besloten om de volgende beleidsregels met betrekking tot het bepalen van de hoogte van bestuurlijke boetes vast te stellen:

**HOOFDSTUK 1. ALGEMENE BEPALINGEN**

**Artikel 1. Definities**

In deze beleidsregels wordt verstaan onder:

- a. *Autoriteit Persoonsgegevens*: de Autoriteit persoonsgegevens, bedoeld in artikel 6, eerste lid, van de Uitvoeringswet Algemene verordening gegevensbescherming;
- b. *basisboete*: het bedrag dat de basis vormt voor het bepalen van de hoogte van een op te leggen bestuurlijke boete, vastgesteld binnen de bandbreedte van de aan een overtreding gekoppelde boetecategorie, voordat toepassing is gegeven aan paragraaf 2.6;
- c. *betrokkene*: degene op wie een persoonsgegeven betrekking heeft als bedoeld in artikel 4, onder 1, van de Algemene verordening gegevensbescherming;
- d. *recidive*: de omstandigheid dat ten tijde van het begaan van de overtreding nog geen vijf jaren zijn verstreken sedert het opleggen van een bestuurlijke boete door de Autoriteit Persoonsgegevens aan de overtreder ter zake van eenzelfde of een soortgelijke door die overtreder begane overtreding.

**HOOFDSTUK 2. BEPALEN VAN DE HOOGTE VAN BESTUURLIJKE BOETES**

*Paragraaf 2.1 Overtredingen met een wettelijk boetemaximum van € 10.000.000 respectievelijk € 20.000.000 of, voor een onderneming, tot 2% respectievelijk 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar.*

**Artikel 2. Categorie-indeling en boetebreedtes**

- 2.1 De bepalingen ter zake van overtreding waarvan de Autoriteit Persoonsgegevens een bestuurlijke boete kan opleggen van ten hoogste het bedrag van € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, zijn in bijlage 1 ingedeeld in categorie I, categorie II of categorie III.
- 2.2 De bepalingen ter zake van overtreding waarvan de Autoriteit Persoonsgegevens een bestuurlijke boete kan opleggen van ten hoogste het bedrag van € 20.000.000 of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, zijn in bijlage 2 ingedeeld in categorie I, categorie II, categorie III of categorie IV.
- 2.3 De Autoriteit Persoonsgegevens stelt de basisboete voor overtredingen waarvoor een wettelijk boetemaximum geldt van € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, dan wel € 20.000.000 of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, vast binnen de volgende boetebreedtes:

Categorie	Boetebreedte tussen € 0 en € 200.000	Basisboete: € 100.000
Categorie II	Boetebreedte tussen € 120.000 en € 500.000	Basisboete: € 310.000
Categorie III	Boetebreedte tussen € 300.000 en € 750.000	Basisboete: € 525.000
Categorie IV	Boetebreedte tussen € 450.000 en € 1.000.000	Basisboete: € 725.000

- 2.4 De hoogte van de basisboete wordt vastgesteld op het minimum van de bandbreedte vermeerderd met de helft van de bandbreedte van de aan een overtreding gekoppelde boetecategorie.

Голландский регулятор (Autoriteit Persoonsgegevens) первым в ЕС опубликовал методику расчета и наложения штрафов за нарушения требований законодательства о персональных данных, включая GDPR.

Category	Standard fine bandwidth	Standard penalty
<b>I</b>	EUR 0 – 200.000	EUR 100.000
<b>II</b>	EUR 120.000 – 500.000	EUR 310.000
<b>III</b>	EUR 300.000 – 750.000	EUR 525.000
<b>IV*</b>	EUR 450.000 – 1.000.000	EUR 725.000

\* Only in case the legal maximum penalty of EUR 20.000.000/ 4% turnover applies.

## Методика по расчету и наложению штрафов в Германии (2019.10)

STEP  
1

### Classify company by size

By global annual turnover.

Micro-Enterprises	Small Enterprises	Medium-sized Enterprises	Large Enterprises
Annual turnover less than EUR 2 million	Annual turnover between EUR 2 and 10 million	Annual turnover between EUR 10 and 50 million	Annual turnover more than EUR 50 million
Subgroup 1	Subgroup 1	Subgroup 1	Subgroup 1
Subgroup 2	Subgroup 2	Subgroup 2	Subgroup 2
Subgroup 3	Subgroup 3	Subgroup 3	Subgroup 3
		Subgroup 4	Subgroup 4
		Subgroup 5	Subgroup 5
		Subgroup 6	Subgroup 6
		Subgroup 7	Subgroup 7

Регуляторы из Германии (Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder - DSK) разработали единую методику расчета и наложения штрафов за нарушения требований законодательства о персональных данных, включая GDPR.

Based on the classification, the penalty guidelines suggest the following steps:

STEP  
2

### Determine the average turnover

Determine each subgroup's average annual turnover.

STEP  
3

### Calculate the "daily rate"

By dividing the average turnover (step 2) of a company's subgroup by 360.

STEP  
4

### Determine the severity of offence

Multiply the daily rate by a factor between 1 and 12, depending on the severity of the offence (Art. 83 (2) GDPR).

STEP  
5

### Further considerations

Determine the relevance of any other criteria under Article 83(2) GDPR.



## 721 Методика по расчету и наложению штрафов в Дании (2021.01)



**Bødevejledning**

Udmåling af bøder til virksomheder

Januar 2021

 **DATATILSYNET**

	Kategori 1	Kategori 2	Kategori 3	Kategori 4	Kategori 5	Kategori 6
Grundbeløb - dynamisk bødeloft	> 3,75 mio. kr.	> 7,5 mio. kr.	>15 mio. kr.	> 7,5 mio. kr.	> 15 mio. kr.	> 30 mio. kr.
Grundbeløb - statisk bødeloft	3,75 mio. kr.	7,5 mio. kr.	15 mio. kr.	7,5 mio. kr.	15 mio. kr.	30 mio. kr.

Virksomhedens størrelse	Maksimal justering (ned til)	Kategori 1	Kategori 2	Kategori 3
Meget store virksomheder (omsætning > 500 mio. kr.)		> 3,75 mio. kr.	> 7,5 mio. kr.	> 15 mio. kr.
Store virksomheder (omsætning ≤ 500 mio. kr.)		3,75 mio. kr.	7,5 mio. kr.	15 mio. kr.
Mellemstore virksomheder (omsætning ≤ 375 mio. kr.)	Standard grundbeløb x 0,1	≥ 375.000 kr.	≥ 750.000 kr.	≥ 1,5 mio. kr.
Små virksomheder (omsætning ≤ 75 mio. kr.)	Standard grundbeløb x 0,02	≥ 75.000 kr.	≥ 150.000 kr.	≥ 300.000 kr.
Mikro virksomheder (omsætning ≤ 15 mio. kr.)	Standard grundbeløb x 0,004	≥ 15.000 kr.	≥ 30.000 kr.	≥ 60.000 kr.

Virksomhedens størrelse	Maksimal justering (ned til)	Kategori 4	Kategori 5	Kategori 6
Meget store virksomheder (omsætning > 500 mio. kr.)		> 7,5 mio. kr.	> 15 mio. kr.	> 30 mio. kr.
Store virksomheder (omsætning ≤ 500 mio. kr.)		7,5 mio. kr.	15 mio. kr.	30 mio. kr.
Mellemstore virksomheder (omsætning ≤ 375 mio. kr.)	Standard grundbeløb x 0,1	≥ 750.000 kr.	≥ 1,5 mio. kr.	≥ 3 mio. kr.
Små virksomheder (omsætning ≤ 75 mio. kr.)	Standard grundbeløb x 0,02	≥ 150.000 kr.	≥ 300.000 kr.	≥ 600.000 kr.
Mikro virksomheder (omsætning ≤ 15 mio. kr.)	Standard grundbeløb x 0,004	≥ 30.000 kr.	≥ 60.000 kr.	≥ 120.000 kr.



Datu valsts inspekcija

## ADMINISTRATĪVO NAUDAS SODU APMĒRA NOTEIKŠANAS KRITĒRIJI UZŅĒMUMIEM UN FIZISKĀM PERSONĀM.

Gadījumos, kad Datu valsts inspekcijā (turpmāk- DVI) par piemērotāko korektīvo līdzekli, kas piemērojams pārzinim vai apstrādātājam par Vispārīgās datu aizsardzības regulas (VDAR) pārkāpumu, tiek izvēlēts administratīvais naudas sods, DVI, nosakot naudas soda apmēru konkrētajā gadījumā, ir jāņem vērā vairāki likumā noteikti kritēriji un apstākļi. Šī mehānisma publicēšanas mērķis panākt konsekventi DVI piemēroto naudas sodu apmēru, padarīt efektīvāku lēmumu pieņemšanas procesu apstrādātājiem kā arī datu subjektu atklātāku un paredzamāku uz tiem attiecināma sodu apmēra noteikšanas mehānismu. Tāpat, šī mehānisma publicēšanai, DVI ieskatā būs preventīva ietekme, jo pārzinim un apstrādātājiem tiks sniegts priekšstats par VDAR pārkāpuma iespējamajām sekām.

### I. Mehānisma piemērošanas jomas

Administratīvos pārkāpumus, par tiem piemērojamos sodus un amatpersonu kompetenci administratīvo pārkāpumu procesā iestādē, ievērojot AAL paredzētos administratīvās atbildības pamatnoteikumus, nosaka attiecīgo nozari regulējošajos likumos vai pašvaldību saistošajos noteikumos.<sup>1</sup> Personas datu aizsardzības jomā ir Vispārīgās datu aizsardzības regula, Fizisko personu datu apstrādes likums un likums "Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā". Šis administratīvo naudas sodu apmēra noteikšanas mehānisms attiecas tikai uz VDAR pārkāpumiem, ko pieļāvuši pārzini vai apstrādātāji- uzņēmumi vai fiziskas personas. Šis administratīvo naudas sodu apmēra noteikšanas mehānisms neattiecas uz sodiem valsts un pašvaldību iestādēm kā arī likuma "Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā" pārkāpumiem.

### II. Administratīvo sodu apmēra noteikšanā piemērojamās normatīvo aktu prasības

Administratīvais pārkāpums ir personas prettiesiska, vainojama rīcība (darbība vai bezdarbība), par kuru likumā vai pašvaldību saistošajos noteikumos paredzēta administratīvā atbildība.<sup>2</sup> Administratīvais sods ir ietekmēšanas līdzeklis, kas tiek piemērots administratīvo pārkāpumu izdarījušajai personai, lai aizsargātu sabiedrisko kārtību, atjaunotu taisnīgumu, sodītu par izdarīto pārkāpumu, kā arī atturētu administratīvo pārkāpumu izdarījušo personu un citas personas no turpmākas administratīvo pārkāpumu izdarīšanas.<sup>3</sup>

Normatīvo aktu pamatojums	Apstākļi	Punktu skaits no	Punktu skaits līdz	Detalizēts novērtējums un komentāri					
VDAR 83(2) a)	Skarto datu subjektu skaits	-2	5	-2	1				
				-1	2 līdz 10				
				0	11 līdz 50				
				1	51 līdz 100				
				2	100 līdz 250				
				3	250 līdz 500				
4	500 līdz 1000								
5	1000 un vairāk								
VDAR 83(2) g)	Skarto personas datu kategoriju skaits	-1	1	-1	1				
				0	2 līdz 5				
				1	5 un vairāk				
VDAR 83(2) g)	Skarto personas datu kategorijas	-2	5	-2 līdz 2	Nav skarti bērni vai īpašo kategoriju personas dati				
				2 un vairāk	Katrā situācijā, kad skarti bērni personas dati				
				3 un vairāk	Katrā situācijā, kad skarti īpašo kategoriju personas dati				
VDAR 82(2) e)	Iespējamā iepriekšēji pārzina vai apstrādātāja VDAR pārkāpumu skaits	0	2	0	Iepriekšējo pārkāpumu nav				
				1	Viens iepriekšējs pārkāpums ar citu būdību				
				2	Atkārtots pārkāpums par to pašu būdību				
VDAR 83.2(h) AAL 20(1)(4)	Veids, kādā uzraudzības iestāde uzzināja par pārkāpumu, vai un kādā apjomā par pārkāpumu ziņoja pārzinis vai apstrādātājs/ Vai pie atbildības saucamā persona labprātīgi pievienojās pirms izdarītā pārkāpuma atklāšanas	-2	2	-2	Pārzina vai apstrādātāja nekavējoties ziņojums par pārkāpumu pilnā apmērā				
				-1	Pārzina vai apstrādātāja ziņojums saprātīgā termiņā par pārkāpumu pilnā apmērā				
				0	Novēlots pārzina vai apstrādātāja ziņojums pilnā vai nepilnā apmērā				
				0	Pārzina vai apstrādātāja ziņojums saprātīgā termiņā nepilnā apmērā				
				1	Neliels skaits vai viena datu subjekta šūdzība, kam sekojis arī pārzina vai apstrādātāja ziņojums pilnā vai nepilnā apmērā				
				1	Neliels skaits vai viena datu subjekta šūdzība				
				2	Ievērojams skaits datu subjekta šūdzību, kam sekojis arī pārzina vai apstrādātāja ziņojums pilnā vai nepilnā apmērā				
				2	Ievērojams skaits datu subjekta šūdzību bez paziņojuma				
				VDAR 83.2 i) AAL 21(1)	Pārzina vai apstrādātāja rīcība, lai mazinātu kaitējumu datu subjektam/ pie atbildības saucamā persona labprātīgi atbildzinājusi zaudējumu vai novērsusi nodarīto kaitējumu	-4	1	-4	Pēc pārkāpuma nav sekoyusi nekāda rīcība kaitējuma novēršanai
								-3	Pēc pārkāpuma nekavējoties sekoyusi efektīva un visaptveroša rīcība kaitējuma novēršanai, un ir labprātīgi pilnīgi vai daļēji atīdzinātn zaudējumi (ja tādi pastāv un ir konkrēti novērtējami)
-2 līdz -1	Pēc pārkāpuma nekavējoties sekoyusi efektīva bet ne visaptveroša rīcība kaitējuma novēršanai								
0	Pēc pārkāpuma ar novēlošanos sekoyusi efektīva rīcība kaitējuma novēršanai								
1	Pēc pārkāpuma ar novēlošanos sekoyusi neefektīva vai ierobežota rīcība kaitējuma novēršanai								
1	Pēc pārkāpuma nav sekoyusi nekāda rīcība kaitējuma novēršanai								
VDAR 83.2 f)	Sadarbības pakāpe ar uzraudzības iestādi	-2	2	Visa pārējā pārzina vai apstrādātāja rīcība izņemot rīcību, lai mazinātu kaitējumu datu subjektam un atīdzības izmaksa - jau izvērtā iepriekšējn kritērijā.					
AAL 20(1)(1)	Vai uzraudzības iestāde sakārā ar konkrēto pārkāpumu pret pārzini vai apstrādātāju ir vērsusi kādas korektīvās pilnvaras (VDAR	0	2	0	Nekādas korektīvās pilnvaras nav vērstas				
				1	Korektīvās pilnvaras ir vērstas, ir sekoyusi pārzina rīcība, bet tā ir bijusi nepietiekama				
				2	Korektīvās pilnvaras ir vērstas vairākas reizes, ir sekoyusi pārzina rīcība, bet tā ir nepietiekama				

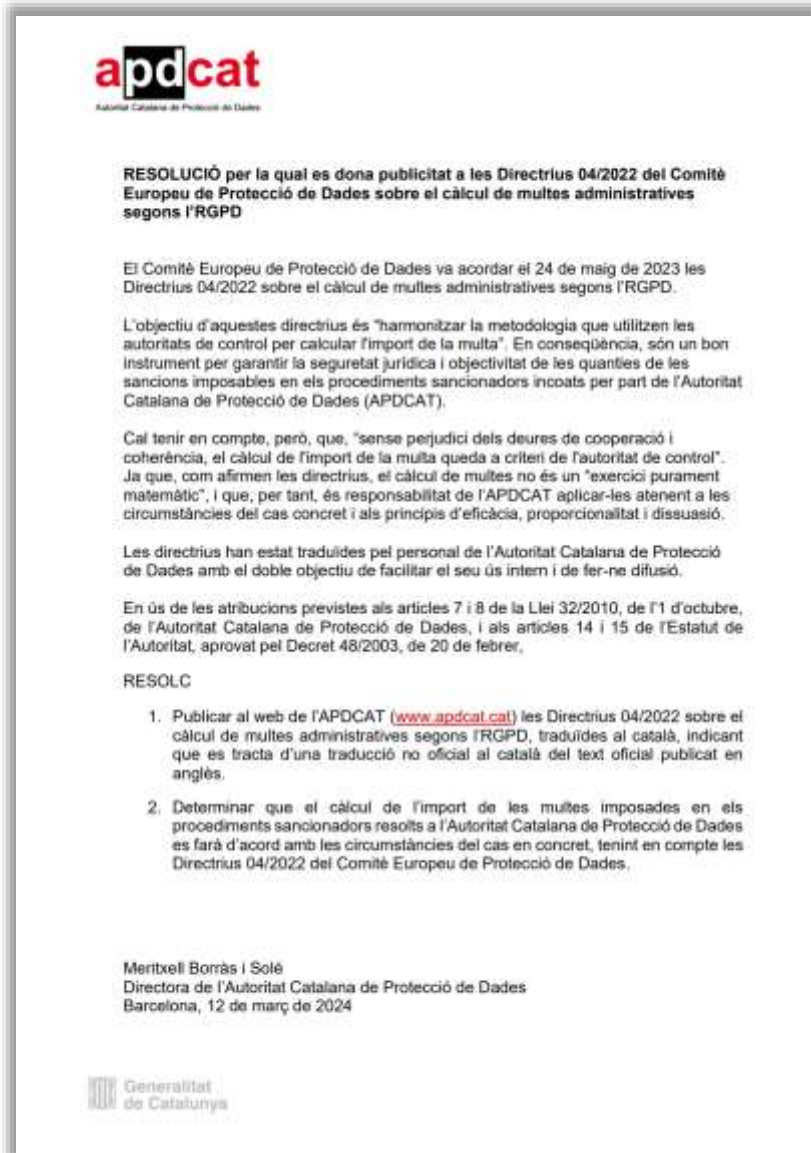
## 723 Методика по расчету и наложению штрафов в Великобритании (2024.03)



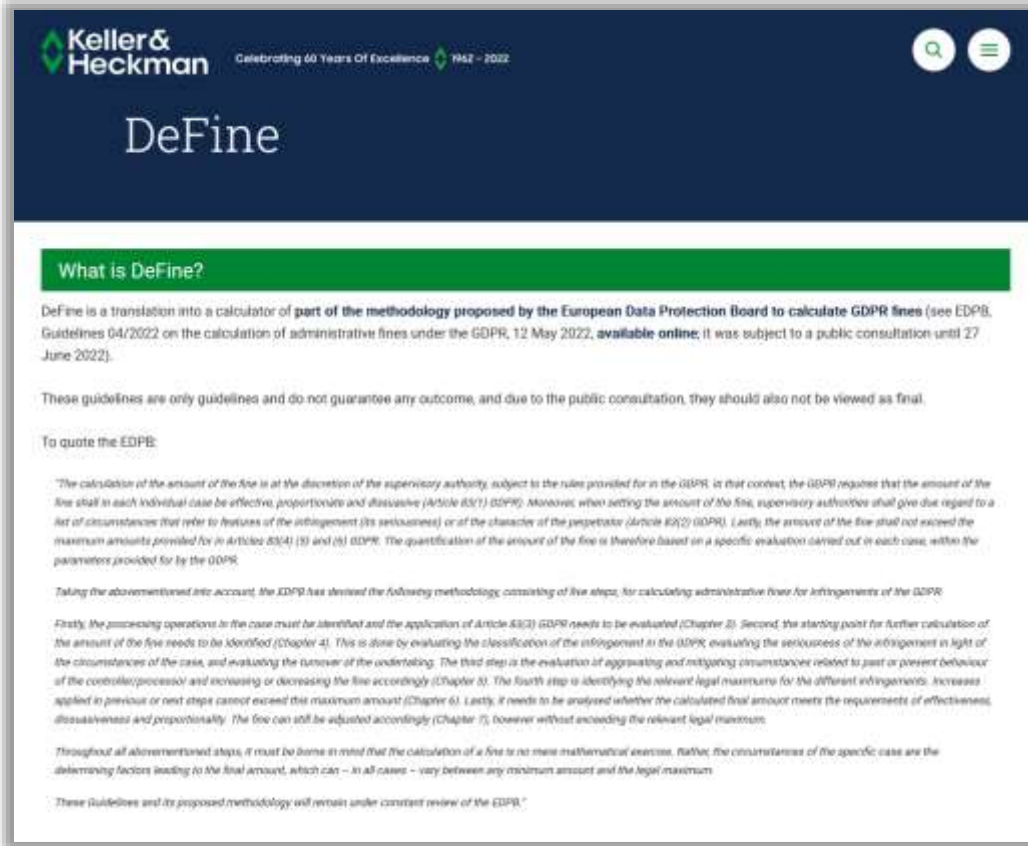
Управление комиссара по информации (ICO) опубликовало новое руководство по штрафам в области защиты данных, в котором подробно описано, как ICO выносит штрафные уведомления и рассчитывает штрафы в соответствии с GDPR и Законом о защите данных 2018 года (DPA 2018).

В частности, в руководстве описывается следующий пятиэтапный подход, который ICO будет использовать для расчета суммы штрафов:

1. оценка серьезности нарушения;
2. учет оборота (если контроллер или процессор является частью предприятия);
3. расчет начальной точки определения размера штрафа с учетом серьезности нарушения и, где это уместно, оборота предприятия;
4. корректировка с учетом любых отягчающих или смягчающих факторов;
5. оценка того, является ли штраф эффективным, соразмерным и сдерживающим.



Каталонский орган по защите данных (APDCAT) адаптировал методику расчета суммы штрафов, налагаемых в соответствии с GDPR, следуя рекомендациям EPDB 04/2022 по расчету административных штрафов в соответствии с GDPR.



**Keller & Heckman** Celebrating 60 Years Of Excellence 1962 - 2022

# DeFine

### What is DeFine?

DeFine is a translation into a calculator of **part of the methodology proposed by the European Data Protection Board to calculate GDPR fines** (see EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, 12 May 2022, **available online**; it was subject to a public consultation until 27 June 2022).

These guidelines are only guidelines and do not guarantee any outcome, and due to the public consultation, they should also not be viewed as final.

To quote the EDPB:

*"The calculation of the amount of the fine is at the discretion of the supervisory authority, subject to the rules provided for in the GDPR. In that context, the GDPR requires that the amount of the fine shall in each individual case be effective, proportionate and dissuasive (Article 83(1) GDPR). Moreover, when setting the amount of the fine, supervisory authorities shall give due regard to a list of circumstances that refer to features of the infringement (its seriousness) or of the character of the perpetrator (Article 83(2) GDPR). Lastly, the amount of the fine shall not exceed the maximum amounts provided for in Articles 83(4) (b) and (c) GDPR. The quantification of the amount of the fine is therefore based on a specific evaluation carried out in each case, within the parameters provided for by the GDPR.*

*Taking the abovementioned into account, the EDPB has devised the following methodology consisting of five steps, for calculating administrative fines for infringements of the GDPR:*

*Firstly, the processing operations in the case must be identified and the application of Article 83(2) GDPR needs to be evaluated (Chapter 2). Second, the starting point for further calculation of the amount of the fine needs to be identified (Chapter 4). This is done by evaluating the classification of the infringement in the GDPR, evaluating the seriousness of the infringement in light of the circumstances of the case, and evaluating the turnover of the undertaking. The third step is the evaluation of aggravating and mitigating circumstances related to past or present behaviour of the controller/processor and increasing or decreasing the fine accordingly (Chapter 5). The fourth step is identifying the relevant legal maximums for the different infringements. Increases applied in previous or next steps cannot exceed the maximum amount (Chapter 6). Lastly, it needs to be analyzed whether the calculated final amount meets the requirements of effectiveness, dissuasiveness and proportionality. The fine can still be adjusted accordingly (Chapter 7), however without exceeding the relevant legal maximums.*

*Throughout all abovementioned steps, it must be borne in mind that the calculation of a fine is no mere mathematical exercise. Rather, the circumstances of the specific case are the determining factors leading to the final amount, which can – in all cases – vary between any minimum amount and the legal maximum.*

*These Guidelines and its proposed methodology will remain under constant review of the EDPB."*

DeFine - это перевод в калькулятор части методики, предложенной Европейским советом по защите данных для расчета штрафов по GDPR (см. EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR), помогает разумно предположить, какой может быть "стартовая сумма" штрафа за нарушение GDPR, при условии, что надзорный орган ЕС примет во внимание все предложения EDPB.



## 727 Штраф за неразграниченные доступа к данным пациентов



### Portuguese Data Protection Authority Imposes 400,000 € Fine on Hospital

The Barreiro Hospital in Portugal was fined 400,000 € by the Portuguese Data Protection Authority CNPD (Comissão Nacional de Protecção de Dados) for non-compliance with the EU General Data Protection Regulation (GDPR) by not separating access rights to patients' clinical data.

The public sector hospital had granted access to patients' clinical data via their system to at least nine persons who are non-medical professionals (social workers). In addition, the CNPD discovered that 985 users with an access role for medical doctors were registered, while there are only 296 physicians working at the hospital. Furthermore, patient data at Barreiro hospital was not separated properly from archived data of another hospital, and access authentication mechanisms were found to be insufficient.

The fines were imposed after the Authority had carried out an inspection at the hospital after having been alerted by the medical association. The CNPD held that the principles of integrity and confidentiality, data minimization in order to limit access to patients' clinical data, and the controller's inability to ensure the confidentiality and integrity of the data in their system (data security) were violated. The first two breaches were considered with 150,000 € each, while the third led to an increase by 100,000 €.

**Кто:** Comissão Nacional de Protecção de Dados (Португалия)

**Кого:** Больница Баррейро

**Когда:** 2018.07

**За что:** нарушение ст. 5(1)(f) и 32 GDPR

**Как:** штраф €400,000

**Причина:** (1) в медицинской информационной системе был доступ к клиническим данным пациентов, по крайней мере, 9 лицам, не являющимся медицинскими работниками (штраф €150,000); (2) в медицинской информационной системе были обнаружены учетные записи 985 пользователей, наделенных правами доступа для врачей, в то время как в больнице работали только 296 врачей (штраф €150,000); (3) персональные данные пациентов не были должным образом отделены от архивных данных другой больницы, а эффективность механизмов аутентификации пользователей была признана недостаточной (штраф €100,000).

## 728 Штраф за неправильно настроенную систему CCTV

**Salzburger Nachrichten**

### Datenschutz: Erste Strafe verhängt

von IRIS BURTSCHER

Die EU-Datenschutzverordnung löste eine Beschwerdeflut aus. Nun hat die Behörde erstmals einen Unternehmer gestraft. Von einer Buße in Millionenhöhe ist man aber weit entfernt.

Mittwoch  
19. September 2018

Facebook Twitter Messenger

Artikel drucken



Es betrifft das Reisebüro ums Eck genauso wie die Netzgiganten Facebook oder Google: Die Datenschutz-Grundverordnung (DSGVO) gibt EU-Bürgern seit Ende Mai mehr Mitsprache dabei, was Unternehmen mit ihren persönlichen Daten machen. Bei Verstößen sind Strafen von bis zu 20 Millionen Euro oder bis zu vier Prozent des Konzernumsatzes möglich.

**Кто:** Österreichische Datenschutzbehörde (Австрия)

**Кого:** букмекерская контора

**Когда:** 2018.09

**За что:** нарушение ст. 5 и 6 GDPR

**Как:** штраф €4,800

**Причина:** неправильно настроенная система внутреннего видеонаблюдения (CCTV), в поле зрения некоторых видеокамер которой попало городское общественное пространство.



## 729 Штраф за отсутствие Controller-to-Processor Agreement



20.01.2019 16:19 Uhr

### DSGVO: 5000 Euro Bußgeld für fehlenden Auftragsverarbeitungsvertrag

Ein kleines Unternehmen wurde mangels Vertrags zur Auftragsverarbeitung zu einem Bußgeld verurteilt. Auslöser war eine Anfrage bei den Datenschutzbehörden.

Von Joerg Heidrich



Seit Anwendung der DSGVO Ende Mai 2018 gab es nur sehr vereinzelt Fälle von Bußgeldern, die von den Aufsichtsbehörden aufgrund von Verstößen gegen den Datenschutz verhängt wurden. Ein erster Verstoß gegen einen Social Media Anbieter wurde Ende des Jahres bekannt. Es deutet allerdings einiges darauf hin, dass diese anfängliche Schonfrist nun vorbei ist.

Ein weiterer Fall wurde nun aus Hamburg bekannt. Dort hatte die Datenschutzbehörde mit Datum vom 17.12.2018 einen Bußgeldbescheid an das kleine Versandunternehmen Kolibri Image versandt und dieses aufgefordert, einen Betrag von 5000 Euro zuzüglich 250 Euro Gebühren zu zahlen. Begründet wird dieser Bescheid nach Art. 83 Abs. 4 DSGVO durch das Fehlen eines Auftragsverarbeitungsvertrags.

**Кто:** Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Германия)

**Кого:** Kolibri Image Regina

**Когда:** 2018.12

**За что:** нарушение ст. 28(3) GDPR

**Как:** штраф €5,000

**Причина:** отсутствие соглашения о поручении обработки персональных данных (Controller-to-Processor Agreement) между указанной компанией и ее контрагентом.

## Штраф за нарушение законодательства о защите прав потребителей в Италии



**Autorità Garante della Concorrenza e del Mercato**

Seguici su: [social media icons]

Cerca

CHI SIAMO | COMPETENZE | AUTORITÀ TRASPARENTE | PUBBLICAZIONI | SERVIZI | MEDIA | EN

Ti trovi in: Home / Media / Comunicati stampa / PS11112 - Uso dei dati degli utenti a fini commerciali: sanzioni per 10 milioni di euro a Facebook

### PS11112 - Uso dei dati degli utenti a fini commerciali: sanzioni per 10 milioni di euro a Facebook

COMUNICATO STAMPA



L'Autorità Garante della Concorrenza e del Mercato, nella riunione del 29 novembre, ha chiuso istruttoria, avviata nel mese di aprile 2018, nei confronti di Facebook Ireland Ltd. e della sua controllante Facebook Inc. per presunte violazioni del Codice del Consumo, irrogando alle società due sanzioni per complessivi 10 milioni di euro.

L'Autorità ha accertato che Facebook, in violazione degli artt. 21 e 22 del Codice del Consumo, induce ingannevolmente gli utenti consumatori a registrarsi nella piattaforma Facebook, non informandoli adeguatamente e immediatamente, in fase di attivazione dell'account, dell'attività di raccolta, con intento commerciale, dei dati da loro forniti, e, più in generale, delle finalità remunerative che sottendono la fornitura del servizio di social network, enfatizzandone la sola gratuità: in tal modo, gli utenti consumatori hanno assunto una decisione di natura commerciale che non avrebbero altrimenti preso (registrazione al social network e permanenza nel medesimo). Le informazioni fornite risultano, infatti, generiche e incomplete senza adeguatamente distinguere tra l'utilizzo dei dati necessario per la personalizzazione del servizio (con l'obiettivo di facilitare la socializzazione con altri utenti "consumatori") e l'utilizzo dei dati per realizzare campagne pubblicitarie mirate.

L'Autorità ha inoltre accertato che Facebook, in violazione degli artt. 24 e 25 del Codice del Consumo, attua una **pratica aggressiva** in quanto esercita un indebito condizionamento nei confronti dei consumatori registrati, i quali subiscono, senza espresso e preventivo consenso - quindi in modo inconsapevole e automatico - la trasmissione dei propri dati da Facebook a siti web/app di terzi, e viceversa, per finalità commerciali. L'indebito condizionamento deriva dall'applicazione di un meccanismo di presunzione del più ampio consenso alla condivisione di dati. La decisione dell'utente di limitare il proprio consenso comporta, infatti, la prospettazione di rilevanti limitazioni alla fruibilità del social network e dei siti web/app di terzi; ciò condiziona gli utenti a mantenere la scelta pre-impostata da Facebook.

Nello specifico, Facebook, attraverso la pre-selezione della funzione "Piattaforma attiva", preimposta l'abilitazione ad accedere a siti web e app esterni con il proprio account Facebook, predisponendo la trasmissione dei dati dell'utente ai singoli siti web/app, in assenza di un consenso espresso da parte dello stesso. Facebook reItera, poi, il meccanismo della pre-selezione in opt out, rispetto ai dati che vengono condivisi, nella fase in cui l'utente accede con il proprio account Facebook a ciascun sito web/app di terzi, inclusi i giochi. L'utente può, infatti, anche in questo caso, solo disabilitare la pre-impostazione sui dati operata da Facebook, senza poter attuare in ordine agli stessi una scelta attiva, libera e consapevole.

In considerazione dei rilevanti effetti della pratica sui consumatori, l'Autorità ha altresì imposto al professionista, ai sensi dell'art. 27, comma 8, del Codice del Consumo, l'obbligo di pubblicare una dichiarazione rettificativa sul sito internet e sull'App per informare i consumatori.

Roma, 7 dicembre 2018

**Kto:** L'Autorità Garante della Concorrenza e del Mercato – Управление по защите конкуренции и рынка (Италия)

**Koro:** Facebook Ireland Ltd. и ее материнская компания Facebook Inc.

**Kогда:** 2018.12

**За что:** нарушение ст. 21 и 22 Codice del Consumo (Кодекса потребителей)

**Kак:** штраф €10,000,000

**Причина:** намеренное введение пользователей Facebook в заблуждение, т.к. при регистрации в социальной сети не осуществляется информирование об обработке пользовательских персональных данных для коммерческих целей. В вину Facebook был поставлен факт не доведения до сведения пользователей различия между использованием персональных данных, необходимых для персонализации услуги (с целью облегчения социализации с другими пользователями социальной сети) и использованием персональных данных для показа персонализированной рекламы и проведения кампаний различного характера.

# CNIL.

To protect personal data, support innovation, preserve individual liberties

DATA PROTECTION | TOPICS | THE CNIL |  

## The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC

21 January 2019

*On 21 January 2019, the CNIL's restricted committee imposed a financial penalty of 50 Million euros against the company GOOGLE LLC, in accordance with the General Data Protection Regulation (GDPR), for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization.*

On 25 and 28 May 2018, the National Data Protection Commission (CNIL) received group complaints from the associations *None Of Your Business* ("NOYB") and *La Quadrature du Net* ("LQDN"). LQDN was mandated by 10 000 people to refer the matter to the CNIL. In the two complaints, the associations reproach GOOGLE for not having a valid legal basis to process the personal data of the users of its services, particularly for ads personalization purposes.

### The handling of the complaints by the CNIL

The CNIL immediately started investigating the complaints. On 1<sup>st</sup> June 2018, in accordance with the provisions on European cooperation as defined in the General Data Protection Regulation ("GDPR"), the CNIL sent these two complaints to its European counterparts to assess if it was competent to deal with them. Indeed, the GDPR establishes a "one-stop-shop mechanism" which provides that an organization set up in the European Union shall have only one interlocutor, which is the Data Protection Authority ("DPA") of the country where its "main establishment" is located. This authority serves as "lead authority". It must therefore coordinate the cooperation between the other Data Protection Authorities before taking any decision about a cross-border processing carried out by the company.

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Google LLC

**Когда:** 2019.01

**За что:** нарушение ст. 4, 5, 6, 13, 14 GDPR

**Как:** штраф €50,000,000

**Причина:** CNIL по коллективной жалобе 10 тыс. человек провел расследование в отношении Google и оштрафовал компанию за нарушение требований в части доступности пользователям информации об обработке их персональных данных и надлежащего получения их согласий для обработки персональных данных в целях персонализации рекламы.

## Штраф за нарушение принципа «ограничения целью» (purpose limitation)



**Datatilsynet**

Rettigheter og plikter | Personvern på ulike områder | Regelverk og verktøy

Aktuelt

### Varsel om gebyr til Tolldirektoratet

Datatilsynet har i dag varslet Tolldirektoratet om at de kan bli ilagt et overtredelsesgebyr på 900 000 kroner. Tilsynet mener etaten har brutt personopplysningsloven gjennom innsamling og bruk av opplysninger fra kameraer uten lov.

Gebyret er utmålt etter den gamle personopplysningsloven, siden lovbruddene skjedde før den nye personvernforordningen (GDPR) trådte i kraft i juli i fjor. Mangelfulle tekniske og organisatoriske rutiner hos etaten har ført til at tilsynet varsler det høyeste gebyret som er ilagt etter den gamle loven.

#### Har registrert norske borgere uten lov

Datatilsynet har lagt vekt på at Tolldirektoratet har overvåket 80 millioner passeringer, hvor antall berørte personer anslås til 7-8 millioner. Tolletaten skal drive overvåking av grensekryssende trafikk, men de har også registrert og lagret data fra kameraer som Statens Vegvesen har utplassert mange steder i landet. Dette er kameraer som Tolldirektoratet ikke skal ha tilgang til opplysninger fra.

- Det må særlig forventes at en offentlig etat forholder seg til de lovhjemlene de skal forvalte, og evner å rette opp i forholdene raskt. Dette har ikke skjedd, og det er nødvendig med en reaksjon. Vi skal ha tillitt til offentlig forvaltning og særlig dem som utøver kontroll, sier Bjørn Erik Thon.



**Kontaktperson**

 Janne Stang Dahl  
kommunikasjonsdirektør

Kontor: [+47 22 39 69 03](tel:+4722396903)  
Mobil: [+47 97 08 11 20](tel:+4797081120)  
E-post: [janne@datatilsynet.no](mailto:janne@datatilsynet.no)

Publisert: 12.03.2019

**Кто:** Datatilsynet (Норвегия)

**Кого:** Tolldirektoratet (Таможенное управление Норвегии)

**Когда:** 2019.03

**За что:** нарушение ст. 5(1)(b) GDPR

**Как:** возможный штраф €90,000. Итоговая сумма штрафа была [определена 20.11.2020](#) в размере €40,000.

**Причина:** незаконная обработка информации со стационарных и мобильных камер, которые фиксируют автомобильный трафик по всей стране, но который нельзя охарактеризовать как трансграничный. Следовательно, такая обработка персональных данных не может рассматриваться как осуществляемая в целях исполнения таможенного законодательства.

## Штраф за нарушение принципа «минимизации объема данных» (data minimization)



**DATATILSYNET**

GENERELT OM DATABESKYTTELSE ▾ EMNER ▾ TILSYN OG AFGØRELSESR ▾

Du er her: Forside / Tilsyn og afgørelser / Afgørelser / 2019 / mar /  
Tilsyn med Taxa 4x35's behandling af personoplysninger

### Tilsyn med Taxa 4x35's behandling af personoplysninger

Publiceret 18-03-2019 Afgørelse Private virksomheder

Knap 9 mio. personhenførbare taxature er blevet gemt uden et sagligt formål, vurderer Datatilsynet.

Journalnummer: 2018-41-0016

#### Resume

Datatilsynet var i efteråret 2018 på et tilsynsbesøg hos Taxa 4x35, hvor der bl.a. blev set på, om taxaselskabet har fastsat frister for sletning af kundenes oplysninger - og om fristerne bliver efterlevet.

Ifølge Taxa 4x35 anonymiseres de oplysninger, der anvendes til kundens bestilling og afvikling af taxature, efter to år, da der herefter ikke længere er behov for at kunne identificere kunden.

Det er imidlertid kun kundens navn, der slettes efter de to år - men ikke kundens telefonnummer. Oplysninger om kundens taxature (herunder opsamlings- og afleveringsadresser) kan derfor fortsat henføres til en fysisk person via telefonnummeret, som først slettes efter fem år.

**Кто:** Datatilsynet (Дания)

**Кого:** Таха 4x35

**Когда:** 2019.03

**За что:** нарушение ст. 5(1)(e) и 6 GDPR

**Как:** штраф €161,000, дело передано в полицию

**Причина:** компания при обезличивании персональных данных удаляла только имя/фамилию клиента, но номер телефона хранился в базе для обеспечения корректной работы системы. По номеру телефона можно было отследить поездку клиента и адрес. Таким образом, более 8 млн. записей, содержащих персональные данные, продолжали храниться в компании.

## Штраф за непредоставление информации при получении персональных данных не от субъекта данных

Urząd Ochrony Danych Osobowych

Infolinia Urzędu 606-950-000 Wpisz frazę której szukasz

Prezes i Urząd Prawo Edukacja Współpraca Wydarzenia

Aktualności

### Prezes UODO nałożyła pierwszą karę pieniężną

Za niedopełnienie obowiązku informacyjnego Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożyła pierwszą karę w wysokości ponad 943 tys. zł.

- Administrator miał świadomość o ciąży na nim obowiązku informacyjnym. Stąd decyzja o nałożeniu na ten podmiot kary w tej wysokości - podkreśliła Prezes UODO dr Edyta Bielak - Jomaa

Bardzo wiele osób, których dane przetwarzają ukarana spółka, nie miało o tym pojęcia. Administrator ich o tym nie powiadomił. Tym samym odebrał im możliwość skorzystania z praw, jakie przysługują im na gruncie RODO, czyli ogólnego rozporządzenia o ochronie danych. Nie mogli więc one np. sprzeciwić się dalszemu przetwarzaniu ich danych, żądać ich sprostowania czy usunięcia. Prezes UODO uznała, że stwierdzone naruszenie ma poważny charakter, gdyż dotyczy podstawowych praw i wolności osób, których dane przetwarza spółka, jak również dotyczy jednej z podstawowych kwestii, jaką jest informacja o tym, że dane są przetwarzane. Nałożenie kary pieniężnej jest niezbędne, gdyż administrator nie przestrzega przepisów prawa.



Jak wyjaśniał Piotr Drobek, Dyrektor Zespołu Analiz i Strategii w UODO - Spółka nie dopełniała obowiązku informacyjnego w stosunku do ponad 6 mln osób. Spośród około 90 tys. osób których spółka poinformowała o przetwarzaniu danych ponad 32 tys. wniosło sprzeciw wobec przetwarzania ich danych. Pokazuje to jak ważne jest prawidłowe spełnienie obowiązków informacyjnych dla realizacji uprawnień przysługujących nam zgodnie z RODO.

Decyzja Prezes UODO dotyczyła postępowania związanego z działalnością spółki, która przetwarzała dane osób pozyskane ze źródeł publicznie dostępnych, m.in. z Centralnej Ewidencji i Informacji Działalności Gospodarczej (CEiDG), i przetwarzała je w celach zarobkowych. Organ weryfikował niedopełnienie obowiązku informacyjnego wobec osób fizycznych prowadzących działalność gospodarczą - przedsiębiorców, którzy aktualnie ją prowadzą bądź tę działalność zawiesili, jak i o tych, którzy prowadzili ją w przeszłości. Administrator spełnił obowiązek informacyjny, podając informacje wymagane przepisami art. 14 ust. 1-3 RODO jedynie wobec tych osób, do których miał adresy e-mail. W przypadku pozostałych osób tego nie zrobił - jak sam to wyjaśniał w toku postępowania - z uwagi na wysokie koszty takiej operacji. Dlatego jedynie na swojej stronie internetowej zamieścił kluczową informację.

W ocenie Prezes UODO takie działanie było niewystarczające - mając dane kontaktowe do poszczególnych osób powinien spełnić wobec nich obowiązek informacyjny, poinformować m.in. o swoich danych, skąd ma dane tych osób, w jakim celu i jak długo zamierza je przetwarzać oraz o przysługujących osobom prawach na gruncie RODO.

**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** частная компания

**Когда:** 2019.03

**За что:** нарушение ст. 14(1)-(3) GDPR

**Как:** штраф €220,000

**Причина:** компания не предоставила необходимую информацию субъектам при получении персональных данных не от них самих в отношении 6,000,000 субъектов, так как компания располагала только их почтовыми адресами/номерами телефонов и посчитала слишком дорогостоящим использование таких каналов коммуникации.

## Штраф за неправомерную обработку персональных данных бывших клиентов

DER TAGESSPIEGEL

Verstöße gegen Datenschutz 23.05.2019, 15:29 Uhr

### 50.000 Euro Bußgeld gegen Onlinebank N26

Es ist eine der bislang höchsten Strafen wegen Verstößen gegen die Datenschutzgrundverordnung: N26 führte wohl eine „schwarze Liste“ mit Daten von Ex-Kunden. VON OLIVER VOSS



Neuer Ärger für den Gründer der N26 Bank, Valentin Staff. FOTO: WOLFGANG KLUMPPA

Die Berliner Datenschutzbeauftragte hat mit 50.000 Euro eine der bislang höchsten Strafen wegen Verstößen gegen die Datenschutzgrundverordnung (DSGVO) verhängt. Betroffen ist dabei nach Informationen des Fachdienstes „Tagesspiegel Background Digitalisierung & KI“ die **Onlinebank N26**. „Ein Bußgeld betrug 50.000 Euro und betraf die unbefugte Verarbeitung personenbezogener Daten ehemaliger KundInnen und Kunden durch eine Bank“, erklärt die Behörde. Den Namen will sie nicht nennen.

Das Unternehmen soll zahlen, weil Daten ehemaliger Kunden auf einer Art „schwarzer Liste“ gespeichert wurden. Dies ist jedoch nur für Kunden die unter Geldwäscheverdacht stehen zulässig. Die Betroffenen konnten dadurch keine neuen Konten eröffnen. Inzwischen wurde die Praxis nach Angaben von N26 geändert, „so dass sich jetzt ehemalige Kunden, die nicht geldwäscheverdächtig sind, neu anmelden können“. N26 geht rechtlich gegen das Bußgeld vor und wollte sich mit Verweis auf das laufende Verfahren nicht weiter äußern.

**Кто:** Berliner Datenschutzbeauftragte (Германия)

**Кого:** Tagesspiegel Background Digitalisierung & KI, представляющую сервисы с использованием бренда «Smartphone-Bank N26»

**Когда:** 2019.05

**За что:** нарушение ст. 6 GDPR

**Как:** штраф €50,000

**Причина:** неправомерная обработка персональных данных бывших клиентов компании, некоторые из которых были зафиксированы в некоем «черном списке».

## Штраф за неправомерную обработку персональных данных в избирательных целях



The screenshot shows the EDPB website with the following content:

**First Belgian GDPR fine**  
 Tuesday, 28 May 2019

On Tuesday 28 May 2019, the Belgian DPA imposed its first financial penalty since the entry into application of the GDPR. The administrative fine amounts to EUR 2 000 and concerns the misuse of personal data for election purposes. Although the fine is modest, the message is not: Data protection is an important matter to us all, but data controllers must assume their responsibility, especially if they have a government mandate.

**L'Autorité de protection des données prononce une sanction dans le cadre d'une campagne électorale**

Ce mardi 28 mai 2019, (Autorité de protection des données (APD)) a prononcé sa première sanction financière depuis l'entrée en vigueur du RGPD. L'amende administrative imposée s'élève à 2000 euros et vise l'utilisation abusive de données personnelles par un bourgmestre à des fins de campagne électorale. Si l'amende est modérée, son message est important : la protection des données est l'affaire de tous, et les responsables de traitement doivent prendre leurs responsabilités, surtout quand ils détiennent un mandat public.

**L'affaire : envoi de courriel électoral personnalisé par un mandataire public**

L'APD a reçu une plainte concernant l'utilisation par un bourgmestre de données obtenues dans le cadre de l'exécution de sa fonction à des fins de campagne électorale.

Les plaignants étaient entrés en contact avec le bourgmestre de la commune via leur architecte dans le cadre d'une modification de lotissement. L'architecte avait, à cette occasion, contacté le bourgmestre par courrier électronique avec en copie les adresses email des plaignants. La veille des élections communales du 14 octobre 2018, le bourgmestre avait alors utilisé la fonction « Reply » de l'email afin d'envoyer un message électoral aux plaignants.

Les deux parties ont été entendues par la Chambre Contentieuse de l'APD ce 28 Mai 2019. Suite à cette audition, la chambre a conclu qu'une infraction au RGPD avait bien été commise.

**Non-respect du principe de finalité en protection des données**

Le Règlement général sur la protection des données (RGPD) précise que les données collectées par un responsable de traitement (dans ce cas-ci : les adresses emails obtenues par le bourgmestre) doivent être collectées pour des finalités déterminées et ne pouvant être traitées ultérieurement de manière incompatible avec les finalités en question. La réutilisation de données obtenues dans le cadre d'un projet urbanistique à des fins de campagne électorale contrevient donc à ce principe de finalité et constitue une infraction au RGPD.

**Кто:** l'Autorité de protection des données (Бельгия)

**Кого:** мэр одного из муниципалитетов

**Когда:** 2019.05

**За что:** нарушение ст. 5(1)(b) и 6 GDPR

**Как:** штраф €2,000

**Причина:** использование персональных данных, полученных в ходе исполнения должностных обязанностей: переписка с заявителями посредством электронной почты использовалась для их уведомления о предстоящих муниципальных выборах. Размер штрафа небольшой ввиду ограниченного числа "потерпевших" и малого ущерба для прав субъектов.



## Штраф за нарушение принципа «проектируемая защита данных» (privacy by design)

**Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal**  
 Protecția Datelor | Data Protection | Protection des Données

Informații generale | Legislație | Proceduri | Relații Internaționale | Contact

Home + Comunicat\_amenda\_Unicredit 8/07/2019 19:04 Română | English | Français

### PRIMA AMENDĂ ÎN APLICAREA RGPD

Pe data de 27.06.2019, **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal** a finalizat o investigație la operatorul **UNICREDIT BANK S.A.**, și a constatat că acesta a încălcat prevederile art. 25 alin. (1) din **Regulamentul (UE) 2016/679** al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

**Operatorul a fost sancționat contravențional cu amendă în cuantum de 613.912 lei, echivalentul în euro al sumei de 130.000 euro.**

Sancțiunea a fost aplicată UNICREDIT BANK S.A. ca urmare a neaplicării măsurilor tehnice și organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele RGPD și a protejeze drepturile persoanelor vizate. Aceasta a condus la devăluirea în documentele ce conțin detaliile tranzacțiilor și care sunt puse on-line la dispoziția clienților beneficiari ai plăților, a datelor privind CNP-ul și adresa plătorului (pentru situațiile în care plătorul efectua tranzacția dintr-un cont deschis la o altă instituție de credit - tranzacții externe și depuneri la casierie), respectiv a datelor privind adresa plătorului (pentru situațiile în care plătorul efectua tranzacția dintr-un cont deschis la UNICREDIT BANK SA - tranzacții interne), pentru un număr de 337.042 persoane vizate, în perioada 25 mai 2018 - 10.12.2018.

Sancțiunea a fost aplicată ca urmare a unei sesiuni a Autorității Naționale de Supraveghere din data de 22.11.2018 prin care se semnala faptul că datele privind CNP-ul și adresa persoanelor care efectuau plăți la UNICREDIT BANK S.A., prin intermediul tranzacțiilor on-line, erau devăluite către beneficiarul tranzacției, prin formularele de extras de cont/detalii.

Potrivit art. 5 alin. 1 lit. c) din RGPD ("Principii legate de prelucrarea datelor cu caracter personal"), operatorul avea obligația de a prelucra date limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate datele.

În același timp, considerentul (78) din Regulament precizează: "Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să respecte în special principiul protecției datelor începând cu momentul concepției și cel al protecției implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, transparența în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranță și să le îmbunătățească. Atunci când elaborează, proiectează, selectează și utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucresc date cu caracter personal pentru a-și îndeplini rolul, producătorii acestor produse și furnizorii acestor servicii și aplicații ar trebui să fie încurajați să aibă în vedere dreptul la protecția datelor la momentul elaborării și proiectării unor astfel de produse, servicii și aplicații și, ținând cont de stadiul actual al dezvoltării, să se asigure că operatorii și persoanele împuternicite de operatorii sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor. Principiul protecției datelor începând cu momentul concepției și cel al protecției implicite a datelor ar trebui să fie luate în considerare și în contextul licitațiilor publice."

**Biroul juridic și comunicare**  
A.N.S.P.D.C.P.

**Кто:** Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Румыния)

**Кого:** Unicredit Bank

**Когда:** 2019.06

**За что:** нарушение ст. 25(1) GDPR

**Как:** штраф €130,000

**Причина:** банк спроектировал систему платежей таким образом, что персональные данные (место жительства и личный номер) сотен тысяч плательщиков были раскрыты получателям платежа в нарушение принципа минимизации данных. Нарушение произошло в результате недобросовестной работы инженеров, системных архитекторов, спроектировавших систему и не исключивших возможность передачи получателям избыточных сведений.

## Штраф за нарушение принципа «ограничения срока обработки» (storage limitation)



  
**DATATILSYNET**

### Møbelfirma indstillet til bøde

Publiceret 11-06-2019  
Nyhed

Datatilsynet har politianmeldt IDdesign A/S og indstillet virksomheden til en bøde på 1,5 mio kr. for manglende sletning af oplysninger om ca. 385.000 kunder.

I efteråret 2018 var Datatilsynet på tilsynsbesøg hos IDdesign, hvor der bl.a. blev set på, om virksomheden havde fastsat frister for sletning af kundernes oplysninger, og om fristerne blev efterlevet.

#### Ingen slettefrister

Forud for tilsynsbesøget havde IDdesign sendt en oversigt over de systemer, som virksomheden anvender til behandling af personoplysninger. IDdesign oplyste i den forbindelse, at der i enkelte IDEmøbler-butikker fortsat anvendes et ældre system, som ellers er erstattet af et nyere system i de andre butikker, og at der i det gamle system behandles oplysninger om ca. 385.000 kunders navn, adresse, telefonnummer, e-mail og købshistorik. Under tilsynsbesøget oplyste IDdesign endvidere, at der ikke er fastsat slettefrister i dette system, hvorfor personoplysninger i det gamle system aldrig er blevet slettet.

#### Derfor indstilles der til bøde

Det fremgår af databeskyttelsesforordningen, at personoplysninger skal opbevares, så det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

**Кто:** Datatilsynet (Дания)

**Кого:** мебельная компания IDdesign A/S

**Когда:** 2019.06

**За что:** нарушение ст. 5(1)(e) и 5(2) GDPR

**Как:** штраф €201,000




**Причина:** в ходе проведенного 08.10.2018 года аудита был выявлен факт использования компанией IDdesign ERP-систем AX 2.5 и AX 2012, для которых не были определены сроки обработки персональных данных около 385,000 клиентов (ФИО, адрес, номер телефона, адрес электронной почты и история покупок) мебельных магазинов IDE, а также не осуществлялось прекращение обработки персональных данных клиентов после достижения цели их обработки. Кроме того, для системы подбора персонала YoungCRM и системы управления персоналом Timetable не были документированы процедуры уничтожения персональных данных.

## Штраф за неправомерное использование системы видеонаблюдения

MÉDIATHÈQUE | GLOSSAIRE | LEXIQUE FR-EN | BESOIN D'AIDE | PRESSE | [FR](#) - EN | GESTION DES COOKIES

**CNIL.**

*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

MES DÉMARCHES | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL |   

### UNIONTRAD COMPANY : 20 000 euros d'amende pour vidéosurveillance excessive des salariés

*18 juin 2019*

---

*La formation restreinte de la CNIL a prononcé une sanction de 20 000 euros à l'encontre de la société UNIONTRAD COMPANY pour avoir mis en place un dispositif de vidéosurveillance qui plaçait ses salariés sous surveillance constante. Elle a également prononcé une injonction afin que la société prenne des mesures pour assurer la traçabilité des accès à la messagerie professionnelle partagée.*

La société UNIONTRAD COMPANY est une très petite entreprise (TPE) composée de neuf salariés et spécialisée dans la traduction.

Entre 2013 et 2017, la CNIL a reçu des plaintes de plusieurs salariés de la société qui étaient filmés à leur poste de travail. Elle a, à deux reprises, alerté la société sur les règles à respecter lors de l'installation de caméras sur le lieu de travail, en particulier, qu'il ne fallait pas filmer en continu les salariés et qu'une information sur la présence de caméras devait leur être donnée.

Un contrôle a été mené dans les locaux de la société en février 2018. Il a permis de constater que :

- la caméra présente dans le bureau des six traducteurs les filmait à leur poste de travail sans interruption ;
- aucune information satisfaisante n'avait été délivrée aux salariés ;
- les postes informatiques n'étaient pas sécurisés par un mot de passe et les traducteurs accédaient à une messagerie professionnelle partagée avec un mot de passe unique.

En juillet 2018, la Présidente de la CNIL a mis en demeure la société de se mettre en conformité à la loi Informatique et Libertés, en lui demandant de :

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Uniontrad

**Когда:** 2019.06

**За что:** нарушение ст. 5(1)(с), 12, 13, 32 GDPR

**Как:** штраф €20,000 + по €200 за каждый день задержки в исполнении предписания

**Причина:** неправомерное использование системы видеонаблюдения, которая постоянно контролировала работников. До этого CNIL дважды предупреждала компанию о том, что работники не должны быть постоянными объектами видеосъемки и что им должна быть предоставлена исчерпывающая информация о функционале и целях использования внутренней системы видеонаблюдения.

## Самый большой штраф за нарушение GDPR в Великобритании

Search jobs Sign in Search International edition

**The Guardian**

on Sport Culture Lifestyle More

### BA faces £183m fine over passenger data breach

ICO says personal data of 500,000 customers was stolen from website and mobile app



▲ A British Airways data breach in 2018 compromised customers' credit card information. Photograph: Frank Augstein/AP

British Airways is to be fined more than £183m by the Information Commissioner's Office after **hackers stole the personal data of half a million of the airline's customers.**

The ICO said its extensive investigation found that the incident involved customer details including login, payment card, name, address and travel booking information being harvested after being diverted to a fraudulent website.

**Кто:** Information Commissioner's Office (Великобритания)

**Кого:** British Airways

**Когда:** 2019.07

**За что:** нарушение ст. 32 GDPR

**Как:** заявленный штраф в 2019 году - €204,600,000, [назначенный штраф в 2020 году - €22,038,000](#)

**Причина:** непринятие надлежащих мер защиты персональных данных 500,000 клиентов, доступ к которым получили злоумышленники после взлома корпоративного веб-сайта и мобильного приложения British Airways в июне 2018 года. Размер штрафа составляет 1,5% годового оборота British Airways в 11,6 млрд фунтов стерлингов за 2018 год.

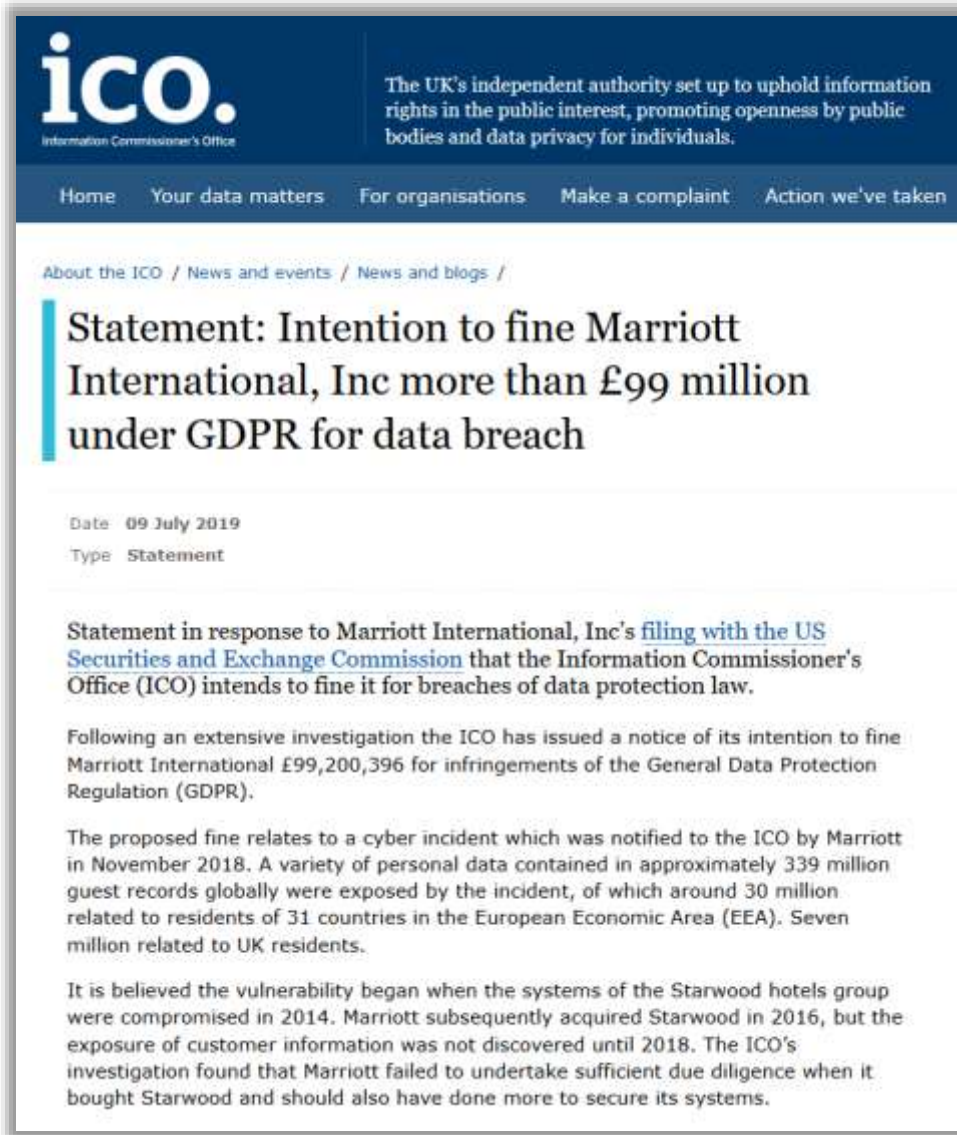
**Последствия:** High Court UK в октябре 2019 г. одобрил подачу группового иска клиентов, пострадавших от утечки данных, против British Airways. У субъектов 15 месяцев на то, чтобы присоединиться к иску и реализовать свое право на компенсацию за причиненный ущерб согласно ст.82 GDPR.

На декабрь 2020 года к иску [присоединилось](#) более 16,000 субъектов.

<https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways>

<https://www.itgovernance.co.uk/blog/british-airways-data-breach-class-action-lawsuit-approved>

## Штраф за самую большую утечку (339 млн. записей) персональных данных



**ico.**  
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters For organisations Make a complaint Action we've taken

About the ICO / News and events / News and blogs /

### Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach

Date: 09 July 2019  
Type: Statement

Statement in response to Marriott International, Inc's [filing with the US Securities and Exchange Commission](#) that the Information Commissioner's Office (ICO) intends to fine it for breaches of data protection law.

Following an extensive investigation the ICO has issued a notice of its intention to fine Marriott International £99,200,396 for infringements of the General Data Protection Regulation (GDPR).

The proposed fine relates to a cyber incident which was notified to the ICO by Marriott in November 2018. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents.

It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.

**Кто:** Information Commissioner's Office (Великобритания)

**Кого:** Marriott International, Inc

**Когда:** 2019.07

**За что:** нарушение ст. 32 GDPR

**Как:** заявленный штраф в 2019 году - €110,390,200, [назначенный штраф в 2020 году - €20,340,000](#)

**Причина:** произошедшая в 2018 году утечка персональных данных, содержащихся примерно в 339 миллионах гостевых записей по всему миру, из которых около 30 миллионов относятся к жителям 31 страны в ЕС/ЕАСТ, включая 7 миллионов жителей Великобритании. Предполагается, что уязвимость возникла в 2014 году в системе бронирования группы отелей Starwood. В 2016 году Marriott приобрела Starwood, но уязвимость не была обнаружена вплоть до 2018 года. Расследование ICO показало, что Marriott не удалось провести надлежащую проверку информационной безопасности систем Starwood с точки зрения обеспечения защиты персональных данных.

## Штраф за необеспечение защиты персональных данных ТВ-звезды



The screenshot shows the website of the Autoriteit Persoonsgegevens (Dutch Data Protection Authority). The header includes the logo and navigation menu. The main content is a news article titled "Haga beboet voor onvoldoende interne beveiliging patiëntendossiers". The article text states that Haga Hospital was fined for inadequate internal security of patient records, with 10 employees accessing medical records of a patient without authorization.

**AUTORITEIT  
PERSOONSgegevens**

Home Actueel Over privacy ▾ Onderwerpen ▾ Zelf doen ▾

Info voor FG's

# Haga beboet voor onvoldoende interne beveiliging patiëntendossiers

Nieuwsbericht / 16 juli 2019

Categorie:  
Beveiliging van persoonsgegevens,  
Zorgverleners en de AVG, Medisch dossier

Het HagaZiekenhuis heeft de interne beveiliging van patiëntendossiers niet op orde. Dit blijkt uit onderzoek van de Autoriteit Persoonsgegevens (AP). Dit onderzoek volgde toen bleek dat tientallen medewerkers van het ziekenhuis onnodig het medisch dossier van een bekende Nederlander hadden ingezien. De AP legt het HagaZiekenhuis voor de onvoldoende beveiliging een boete op van 460.000 euro.

**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** Haga Hospital

**Когда:** 2019.07

**За что:** нарушение ст. 25 и 32 GDPR

**Как:** штраф €460,000

**Причина:** был выявлен факт неправомерного доступа работников госпиталя к персональным данным местной ТВ-звезды, являющийся пациентом госпиталя.

**Предписание:** госпиталь в срок до 02.10.2019 обязан предпринять все необходимые действия для улучшения системы защиты персональных данных. В противном случае, за каждые две недели просрочки госпиталь будет оштрафован на дополнительные €100,000. Максимальный размер такого дополнительного штрафа может составить до € 300,000.

# Штраф за необеспечение защиты персональных данных 6 млн. лиц

РЕПУБЛИКА БЪЛГАРИЯ  
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Начало Институцията Правна рамка Насоки Препитва Контексти

Ползва информация  
Дължностни лица по защита на данните  
Поддаване на жалби и сигнали  
Международни сътрудничества  
Шенгенски програмство  
Анкета

ПРАКТИЧЕСКИ ВЪПРОСИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ СПЕД. 25 МАЙ 2018 Г.

10 ПРАКТИЧЕСКИ СЪВЕТА ЗА ПРИЛАГАНЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ ПРИ ПРИЛАГАНЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

ПРОБЛЕМ НА СОБИРАНЕТО ИЛИ ОБРАБОТКАТА НА ЛИЧНИТЕ ДАННИ В РАМНОУМНОСТТА

Информационни технологии

Нашето > Информация за извършена проверка в Националната агенция за приходите

## Информация за извършена проверка в Националната агенция за приходите

29.06.2019

В хода на извършена в срок от един месец проверка на Националната агенция за приходите (НАП) е установено, че при осъществяване на дейността си, агенцията, в качеството ѝ на администратор на лични данни, не е прилагала подходящи технически и организационни мерки, в резултат на което е осъществил неавторизиран достъп, неразрешено разкриване и разпространение на следните категории лични данни на физически лица: имена, ЕГН и адреси на български граждани, телефони, електронен адреси и друга информация за контакт, данни от годишни данъчни декларации на физически лица, данни от зонираните декларации, данни за здравноосигурителен внос (на не в за недвижимост статус или информация за лечение на гражданите), данни за издадени вноски за административни нарушения, данни за извършени плащания на данъци и осигурителни задължения чрез „Български тощи“ АД, както и данни за платен и възстановен ДДС, платен в чужбина.

Установено е, че в неавторизиран достъп и разпространение в интернет пространството информация си съдържат лични данни на общо 8 074 140 физически лица, което включва 4 104 786 живи физически лица, български и чужди граждани, и 1 959 598 починали физически лица.

С Решение от 23.06.2019 г. КЗПД издала Разпоредба на НАП на основание чл. 28, § 2, Бухал „а“ във връзка с чл. 37, § 1, Бухал „а“ и чл. 83, § 2, Бухал „а“, „б“, „в“, „г“ и „д“ от Регламент (ЕС) 2016/679 за предприемане на подходящи технически и организационни мерки в контекста на действащото законодателство за защита на личните данни, като направи:

- мерки с цел повишаване защитата при обработката на лични данни в приложения за електронни услуги към гражданите;
- извършване на анализ на риска на системите и управлението по обработването, включващи изготвени трасета и функционални задължения за работа на всички информационни системи;
- извършване на оценка на въздействието при идентифициран „висок риск“ за всяка една система и предприемане мерки;
- извършване на оценка на въздействието при първоначално стартиране на нови информационни системи и приложения.

Срещът за изпълнение на разпоредбата е изпратен, съгласно от датата на получаването им.

На 28.06.2019 г., на основание чл. 87, ал. 3 от Закона за защита на личните данни, Венцислав Караджов - Председателят на Комисията за защита на личните данни, издаде Наказателно постановление на НАП за нарушение на чл. 32, § 1, Бухал „б“ от Регламент (ЕС) 2016/679, с оглед осъществяване неавторизиран достъп, неразрешено разкриване и разпространение на лични данни на физически лица от информационните бази данни, поддържащи от агенцията. Извършит на наказателна санкция в 4 104 786 лева.

**Кто:** Комисия за защита на личните данни (България)

**Кого:** Агентство по национальным доходам (Националната агенция за приходите - НАП)

**Когда:** 2019.08

**За что:** нарушение ст. 32(1)(b) GDPR

**Как:** штраф €2,606,780

**Причина:** контролер не принял надлежащих технических данных, выразившееся в неавторизованном доступе, несанкционированном раскрытии и распространении персональных данных 6,074,140 лиц (4,104,786 живых, 1,959.598 умерших).

**Предписание:** в течение 6 месяцев усилить защиту персональных данных при их обработке в приложениях электронных услуг для граждан, выполнить анализ рисков систем и операций обработки, провести оценку воздействия при выявленном «высоком риске» для каждой системы и принять меры, выполнять оценку воздействия перед первичным запуском новых информационных систем и приложений.

## Штраф за обработку биометрических персональных данных несовершеннолетних

The screenshot shows the website of the Swedish Data Inspection Authority (Datainspektionen). The header includes the logo, navigation links (OM OSS, KONTAKTA OSS, PRESS, A-Ö, IN ENGLISH), and a search bar. A red navigation bar contains links for AKTUELLT, VÄGLEDNINGAR, LAGAR OCH REGLER, and UTBILDNINGAR OCH KONFERENSER. The main content area features a breadcrumb trail: Start → Nyheter → Sanktionsavgift för ansiktsgenkänning i skola, published on 2019-08-21. The article title is 'Sanktionsavgift för ansiktsgenkänning i skola'. The text states that the authority has issued a fine of 200,000 SEK to a school for using facial recognition on students. It mentions that the school used the technology for monitoring attendance, and the fine is the first of its kind. The article also notes that the school's actions violated the GDPR and that the fine is 200,000 SEK, which is significant given the school's budget.

**Кто:** Datainspektionen (Швеция)

**Кого:** школа в городе Скеллефтео

**Когда:** 2019.08

**За что:** нарушение ст. 5(1)(с), 9, 35, 36 GDPR

**Как:** штраф €18,630

**Причина:** контролер использовал систему распознавания лиц (в тестовом режиме) для мониторинга посещаемости занятий и обрабатывал биометрические персональные данные с согласия субъектов. Регулятор регулятор счёл, что: для мониторинга посещаемости применение таких технологий является избыточным; согласия на обработку биометрических данных могли быть даны не добровольно (так как ученики зависят от учебного заведения), а иные правовые основания не применимы; не было проведено DPIA, хотя процесс относился к высокорискованным (обработка персональных данных несовершеннолетних, использование новых технологий, обработка биометрических персональных данных).



## Штраф за получение согласий у работников и за нарушение принципа «прозрачности» (transparency)



### SUMMARY OF HELLENIC DPA'S DECISION NO 26/2019

The Hellenic Data Protection Authority, in response to a complaint, conducted an ex officio investigation of the lawfulness of the processing of personal data of the data subjects — employees working at 'PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS LIMITED LIABILITY BUSINESS AND ACCOUNTING SERVICE PROVIDER SA' trading as 'PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS SA' (PWC BS). According to the above complaint the employees were required to provide consent to the processing of their personal data.

The DPA decided that in order for personal data to be processed lawfully, i.e. in compliance with the requirements of the General Data Protection Regulation (GDPR) No 679/2016, all the conditions with regard to the application of and compliance with the principles set out in Article 5(1) of the GDPR should be met.

The identification and choice of the appropriate legal basis under Article 6(1) of the GDPR is closely related both with the principle of fair and transparent processing and the principle of purpose limitation, and the controller must not only choose the appropriate legal basis before initiating the processing -documenting this choice internally in accordance with the principle of accountability-, but also inform the data subject about its use under Articles 13(1)(c) and 14(1)(c) of the GDPR, as the choice of each legal basis has a legal effect on the application of the rights of data subjects.

The principle of accountability constitutes the core of the compliance model adopted by the GDPR. Under this principle, the controller should implement the necessary measures to comply with the principles set out in Article 5(1) of the GDPR and demonstrate their effectiveness, without the DPA having to submit individual — specific questions and requests to assess compliance while exercising its investigative powers.

It should be noted that, due to the fact that this is the initial period of the GDPR's application, the Hellenic DPA submits specific questions and requests, while exercising its investigative powers in order to facilitate the documentation of accountability by controllers.

The principles of lawful, fair and transparent processing of personal data pursuant to Article 5(1)(a) of the GDPR require that consent be used as the legal basis in accordance with Article 6(1) of the GDPR only where the other legal bases do not apply so that once the initial choice has been made it is impossible to swap to a different legal basis. In case the data subject withdraws his or her consent, it is not allowed to carry on the processing of personal data under a different legal basis. Where the legal basis of consent is properly applied, in the sense that no other legal

**Кто:** Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

**Кого:** PricewaterhouseCoopers Business Solutions S.A.

**Когда:** 2019.08

**За что:** нарушение ст. 5(1)(a)(b)(c), 5(2), 6(1)(a), 13(1)(c) и 14(1)(c) GDPR

**Как:** штраф €150,000

**Причина:** PWC BS получала согласие на обработку персональных данных у работников, которое в трудовых правоотношениях не может рассматриваться как свободно данное из-за явного дисбаланса между сторонами. В контексте трудовых отношений выбор согласия в качестве правового основания для обработки персональных данных неуместен, так как такая обработка необходима для исполнения трудовых договоров, соблюдения компанией возложенных на нее обязанностей со стороны действующего законодательства, а также для ведения компанией бесперебойной и эффективной работы, которая является ее законным интересом. Кроме того, PWC BS создала у работников ложное впечатление, что она обрабатывает их персональные данные на законном основании согласия, хотя для такой обработки у компании были иные законные основания.

## Штраф за ненадлежащее обеспечение защиты персональных данных



Urząd Ochrony Danych Osobowych

Wpisz frazę której szukasz

Infolinia Urzędu 606-950-000

Prezes i Urząd    Prawo    Edukacja    Współpraca    Pora

- » Aktualności

### Kara za niewystarczające zabezpieczenia organizacyjne i techniczne

Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) nałożył na spółkę Morele.net karę w wysokości ponad 2,8 mln zł.

Zastosowane przez spółkę środki organizacyjne i techniczne ochrony danych osobowych nie były odpowiednie do istniejącego ryzyka związanego z ich przetwarzaniem, przez co dane około 2 mln 200 tys. osób dostały się w niepowołane ręce. Zabrakło odpowiednich procedur reagowania na wypadek pojawiania się nietypowego ruchu w sieci – uznał Prezes UODO.

Nakładając karę, organ nadzorczy stwierdził, że naruszenie, do którego doszło w tej sprawie, miało znaczną wagę i poważny charakter oraz dotyczyło dużej skali osób. W swojej decyzji organ nadzoru wskazał również, że w wyniku naruszenia powstało wysokie ryzyko negatywnych skutków dla osób, których dane dostały się w niepowołane ręce, jak np. tzw. kradzież tożsamości.



**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** Morele.net

**Когда:** 2019.09

**За что:** нарушение ст. 5, 32 GDPR

**Как:** штраф €645,000

**Причина:** внедрённые компанией меры защиты не покрывали все риски информационной безопасности, связанные с обработкой персональных данных (например, отсутствовали процедуры реагирования на необычную сетевую активность), что было причиной утечки следующих данных 35,000 субъектов: имя, фамилия, номер телефона, электронная почта, адрес доставки, ID номер, доход и тд.

## Штраф за нарушение принципа «проектируемая защита данных» (privacy by design)



The screenshot shows a news article from the European Data Protection Board (EDPS) website. The article is titled "Administrative fines imposed on a telephone service provider" and is dated 7 December 2019. It discusses a case where the Hellenic Data Protection Authority (DPA) imposed fines on the Hellenic Telecommunications Organization (OTE) for breaching the principle of accuracy and data protection by design. The article mentions that OTE deleted entries from its do-not-call register when subscribers requested portability, but failed to properly update its internal systems, leading to unsolicited calls. The DPA found an infringement of Article 25 (data protection by design) and Article 5(1)(c) (principle of accuracy) of the GDPR, imposing a fine of EUR 200,000. A second paragraph discusses a fine for failure to satisfy the right to object, also imposing a fine of EUR 200,000. The article includes a link to the full decision and contact information for the Greek SA.

**Кто:** Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

**Кого:** Hellenic Telecommunications Organization (OTE)

**Когда:** 2019.10

**За что:** нарушение ст. 5(1)(c), 21(3), 25 GDPR

**Как:** штраф €400,000

**Причина:** клиенты Греческой телефонной компании получали рекламные рассылки без возможности отписки. Также клиенты из do-not-call register получали рекламные звонки от сторонних компаний.

## 748 Не только большой штраф, но и компенсация субъекту



**Кто:** Österreichische Datenschutzbehörde (Австрия)

**Кого:** Österreichische Post AG (Почта Австрии)

**Когда:** 2019.10

**За что:** нарушение ст. 6, 9 GDPR

**Как:** штраф €18,000,000 и возбуждение уголовного дела. Федеральный административный суд Австрии, (Bundesverwaltungsgericht) по процессуальным основаниям [26.11.2020 отменил наложенный штраф и закрыл уголовное дело.](#)

**Причина:** Почта использовала адрес и возраст субъектов для определения принадлежности к политическим партиям, а полученные предполагаемые данные продавала третьим лицам. Также почта с целью маркетинга анализировала частоту переездов субъектов.

**Последствия:** Австрийский суд обязал Österreichische Post AG выплатить клиенту компенсацию в €800 (исковое требование было €2,500) за причинённый ущерб ему согласно ст.82 GDPR по причине обработки персональных данных без надлежащего правового основания.

Генеральный адвокат CJEU 06.10.2022 опубликовал свое мнение по делу C-300/21 (UI против Österreichische Post AG) о том, имеет ли истец в деле, рассматриваемом CJEU, право на нематериальные убытки.

[https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority\\_en](https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_en)

<https://www.linkedin.com/pulse/eur-800-non-material-damages-under-art-82-gdpr-court-schweiger/>

<https://noyb.eu/en/analysis-no-non-material-damages-gdpr>

## Штраф за необеспечение безопасности персональных данных при их передаче

**Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal**  
 Protecția Datelor | Data Protec.

Informații generale | Legislație | Proceduri | Relații Internaționale | Contact

Home » Comunicat\_Presa\_09\_10\_2019 20/11/2019 21:18 Română | English | Français

### Noi amenzi în aplicarea RGPD

Autoritatea Națională de Supraveghere a finalizat în data de 01.10.2019 două investigații la operatorii **Raiffeisen Bank S.A.** și **Vreau Credit S.R.L.**, constatând următoarele:

- **Raiffeisen Bank S.A.** a încălcat prevederile **art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din RGPD**, ceea ce a condus la aplicarea unei amenzi contravenționale în cuantumul de 150.000 Euro
- **Vreau Credit S.R.L.** a încălcat prevederile **art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din RGPD**, precum și ale **art. 33 alin. (1) din RGPD**, ceea ce a condus la aplicarea unei amenzi contravenționale în cuantumul de 20.000 Euro.

În ceea ce privește **Raiffeisen Bank S.A.**, Autoritatea Națională de Supraveghere a demarat o investigație, cu urmare a transmiterii de către bancă a unei notificări privind încălcarea securității datelor cu caracter personal prin completarea formularului privind încălcarea securității conform Regulamentului (UE) 2016/679.

Încălcarea securității a constat în faptul că doi angajați ai Raiffeisen Bank S.A., **utilizând datele din documentele de identitate ale unor persoane fizice**, transmise de către angajați ai societății Vreau Credit S.R.L. prin intermediul aplicației mobile WhatsApp, **au efectuat interogări ale sistemului Biroului de Credit** pentru a obține datele necesare în vederea determinării eligibilității la creditare a respectivelor persoane fizice, prin simulări de prescoring. În acest sens, au fost efectuate 1194 simulări, cu privire la 1177 persoane fizice.

De asemenea, pentru 124 de persoane fizice s-a efectuat și consultarea bazei de date a ANAF.

Simulările de prescoring menționate mai sus au fost efectuate prin intermediul aplicației informatice utilizate de Raiffeisen Bank S.A. în activitatea de creditare, iar decizia negativă de creditare a fost comunicată de către angajații Raiffeisen Bank S.A. către angajații Vreau Credit S.R.L., cu încălcarea procedurilor interne.

Sanctiunea a fost aplicată operatorului **cu urmare a faptului că acesta nu a luat măsurile corespunzătoare pentru a se asigura că orice persoană fizică care acționează sub autoritatea acestuia și care are acces la date cu caracter personal, nu le prelucrează decât la cererea sa**, cu excepția cazului în care această obligație revine în termenii dreptului Uniunii sau al dreptului intern.

De asemenea, operatorul nu a implementat **măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător și nu a evaluat riscurile pe care le prezintă prelucrarea.**

Această situație a condus la **accesul neautorizat la datele cu caracter personal prelucrate** prin aplicația informatice utilizată de Raiffeisen Bank S.A. în activitatea de creditare și la **divulgarea neautorizată a datelor cu caracter personal** de către angajați ai băncii.

În ceea ce privește operatorul **Vreau Credit S.R.L.**, acesta a fost sancționat, de asemenea, pentru încălcarea securității datelor, dar și pentru faptul că până la finalizarea investigației nu a notificat autoritatea de supraveghere încălcarea securității datelor cu caracter personal, fără întăzirea nejustificată, deși constatase producerea acestui incident de securitate încă din luna decembrie 2018, ceea ce a condus la încălcarea confidențialității datelor cu caracter personal ale clienților proprii (persoanele vătate) și la prelucrarea neautorizată/ilegală a datelor cu caracter personal ale acestora.

Directia juridică și comunicare  
A.N.S.P.D.C.P.

Sticl

**Кто:** Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Румыния)

**Кого:** Raiffeisen Bank SA

**Когда:** 2019.10

**За что:** нарушение ст. 32 GDPR

**Как:** штраф €150,000

**Причина:** банк проводил скоринговые оценки заемщиков (1,100 субъектов) на основе персональных данных субъектов, зарегистрированных на платформе Vreau Credit. Банк получал данные от Vreau Credit по WhatsApp, а затем возвращал результат Vreau Credit с помощью тех же средств связи.

# Штраф за ненадлежащее ведение RoPA и отсутствие Data Processing Agreement



The screenshot shows the EDPB website with the following content:

**edpb** European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

European Data Protection Board News National News National News The Polish supervisory authority imposed first administrative fine on a public entity

## The Polish supervisory authority imposed first administrative fine on a public entity

Thursday, 21 October 2019 PL

The President of the Personal Data Protection Office ("The President of the Office") imposed first administrative fine of PLN 40,000 on a public entity for failure to comply with the GDPR. The reason for imposing the fine was that the mayor of the city did not conclude a personal data processing agreement with the entities to which he transferred data.

The data processing agreement was not concluded with a company whose servers hosted the resources of the Public Information Bulletin (BIP) of the City Hall in Aleksandrów Kujawski. Such an agreement was also not concluded with another company, which provided software to create BIP and provided service in this area. The President of the Office concluded that Article 28 (3) of the GDPR had been violated. This provision obliges the controller, on behalf of whom personal data processing is performed by another entity, to conclude data processing agreement with him.

As a consequence of the absence of such an agreement, the mayor committed the act of sharing personal data without a legal basis, which violated the principle of lawfulness of processing (Article 5(1)(a) of the GDPR) and the principle of confidentiality (Article 5(1)(f) of the GDPR).

However, these are not the only violations established during the control procedure conducted by the President of the Office. It was also found that there were no internal procedures in place to review the resources available in the BIP in order to determine the timing of their publication. This caused, for example, that in the BIP the property declarations from 2010 were available, among others, while the period of their storage is 6 years, which results from the sectoral regulations. In the case of data whose retention period is not regulated by law, the controller should determine it himself in accordance with the purposes for which he is processing them. Therefore, the controller violated the principle of storage limitation, set forth in Article 5(1)(e) of the GDPR.

It was also established during the investigation that the recorded materials from the city council meetings were available in the BIP only through a link to a dedicated YouTube channel. There were no back-up copies of these recordings at the Municipal Office. Thus, in case of loss of data stored on YouTube, the controller would not have at his disposal the recordings. No risk analysis was carried out for the publication of recordings from board meetings exclusively on YouTube. Thus, the principles of integrity and confidentiality were infringed (Article 5(1)(f) of the GDPR) as well as the principle of accountability (Article 5(2) of the GDPR).

The principle of accountability was also breached in connection with the shortcomings in the register of processing activities. For example, it did not indicate all data recipients, nor did it indicate the planned date of data deletion for certain processing activities.

When imposing a penalty, the President of the Office took into account the fact that despite the irregularities found in the course of the proceedings, the controller did not remove them or implement solutions aimed at preventing future infringements. The controller also did not cooperate with the supervisory authority. Therefore, the President of the Office decided that there were no premises that could mitigate the amount of the fine.

Apart from the financial penalty, the President of the Office also ordered the controller to take action to remedy the relevant infringements within 60 days.

To read the full press release in Polish, [click here](#)

For further information, please contact the Polish DPA: [kancelaria@uodo.gov.pl](mailto:kancelaria@uodo.gov.pl)

**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** орган государственной власти

**Когда:** 2019.10

**За что:** нарушение ст. 5(1)(a), 5(1)(f), 5(1)(e), 5(2), 28(3) GDPR

**Как:** штраф €9,500 и предписание об устранении нарушений за 60 дней

**Причина:** мэр города не заключил Data Processing Agreement с двумя компаниями, которым передавал данные для хостинга системы Public Information Bulletin (BIP) и разработки ПО для BIP. Кроме того, в BIP не соблюдались сроки хранения данных. Также не соблюдался принцип конфиденциальности и целостности в части отсутствия резервирования данных, т.к. записи встреч с заседаний городского совета публиковались только на YouTube. Не был проведен риск-анализ в отношении правомерности публикации этих записей на YouTube. В RoPA (реестр процессов обработки персональных данных) отсутствовала информация о получателях данных, не была указана планируемая дата удаления данных для некоторых процессов.

Αρ. Φακ.: 11.17.001.006.043

25 Οκτωβρίου 2019

**ΑΠΟΦΑΣΗ**

**Βαθμολόγηση αδειών ασθενείας των εργαζοτούμενων στις Εταιρείες Louis χρησιμοποιώντας τον Συντελεστή Bradford**

Αναφέρομαι στην καταγγελία που υποβλήθηκε στο Γραφείο μου αναφορικά με το πιο πάνω θέμα και σε συνέχεια της μεταξύ μας αλληλογραφίας που ήλγει με την επιστολή σας με ημερομηνία 02.09.2019, στην οποία επισυνάψατε την Εκτίμηση του Έννομου Συμφέροντος των πελατών σας, Εταιρείες LGS Handling Ltd, Louis Travel Ltd και Louis Aviation Ltd (στο εξής «οι Εταιρείες Louis») καθώς και με την επιστολή σας με Αρ. Αναρ.: Ε/ΜΜ/Company-8916 και με ημερομηνία 02.09.2019, με την οποία παραθέσατε τις αιτιάσεις των πελατών σας και σας πληροφορώ το ακόλουθο:

**Γενόνοτα**

1.1. Στις 06.06.2018, δόχτηκε παράπονο από το Ελεύθερο Εργατικό Σωματείο Ιδιωτικών Υπαλλήλων ΣΕΚ εναντίον των Εταιρειών Louis, οι οποίες εφαρμόζουν ένα αυτοματοποιημένο σύστημα με σκοπό την διαχείριση, παρακολούθηση και έλεγχο των απουσιών των εργαζοτούμενων για λόγους ασθενείας, χρησιμοποιώντας ένα εργαλείο βαθμολόγησης, γνωστό ως «ο Συντελεστής Bradford» (Bradford Factor). Το εν λόγω σύστημα είναι επίσης προσβάσιμο στο ενδο-δίκτυο των Εταιρειών Louis.

Ο Οργανωτικός Γραμματέας της ΣΕΚ, ανέφερε στην επιστολή του ότι, με δύο επιστολές του προς τον Διευθυντή Ανθρώπινου Δυναμικού, κ. XXXXXXXX, εξέφρασε τη διαφάνια του για τη λειτουργία του εν λόγω συστήματος και τον προέβασε ότι, αν δεν τερματιστεί η λειτουργία του συστήματος, θα ενημερώσει σχετικά το Γραφείο μου.

Όπως σχετικά ανέφερε ο Οργανωτικός Γραμματέας της ΣΕΚ, στην γραπτή απάντηση του προς την ΣΕΚ, ο Διευθυντής Ανθρώπινου Δυναμικού ανέφερε ότι, δεν είχε πρόθεση απενεργοποίησης της λειτουργίας του συστήματος και τον προέβασε/προκάλεσε να προχωρήσει σε γραπτή ενημέρωσή μου.

1.2. Με βάση το καθήκον εξέτασης καταγγελιών που παρέχει στον Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα το άρθρο 57(1)(στ) του Κανονισμού (ΕΕ) 2016/679 (στο εξής «ο Κανονισμός») και το άρθρο 24(β) του Νόμου που προνοεί για την Προστασία των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και για την Ελεύθερη Κυκλοφορία των Δεδομένων Αιτών (Νόμος 125(Ι)/2018), στις 19.07.2018, κατόπιν δικής μου πρωτοβουλίας, πραγματοποιήθηκε συνάντηση στο Γραφείο μου με εκπροσώπους των Εταιρειών Louis για συζήτηση του εν λόγω αυτοματοποιημένου συστήματος.

Παρόντες στη συνάντηση ήταν ο κ. XXXXXXXX, Managing Director των εταιρειών LGS Handling και LOUIS TRAVEL και ο κ. XXXXXX, Διευθυντής Ανθρώπινου Δυναμικού των εταιρειών LGS Handling και LOUIS TRAVEL.

Μεταξύ άλλων, μου ανέφεραν ότι, το σύστημα λειτουργεί με βάση κάποιο αλγόριθμο και αναγνωρίζει ποιοι εργαζοτούμενοι απουσιάζουν συστηματικά από την εργασία τους λόγω ασθενείας.

Ανέφεραν ότι, αντιμετωπίζουν ιδιαίτερο πρόβλημα στο αεροδρόμιο Λάρνακας, όπου λόγω της φύσης της εργασίας (εργασία με σύστημα βάρδιας), αρκετοί εργαζοτούμενοι, ιδιαίτερα τα Σαββατοκύριακα, απουσιάζουν συστηματικά από την εργασία τους και παρουσιάζουν άδεια ασθενείας.

**Κτο:** Γραφείο Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα (Республика Кипр)

**Κοго:** LGS Handling Ltd, Louis Travel Ltd and Louis Aviation Ltd (Louis Group of Companies)

**Κοгда:** 2019.10

**За что:** нарушение ст. 6(1), 9 GDPR

**Как:** штраф €82,000

**Причина:** отсутствие правового основания для обработки персональных данных с использованием ПО «Bradford Factor» в целях оценки больничных работников: так, короткие, частые и незапланированные отлучки приводят к большей дезорганизации в компании, чем более длительные.

По мнению надзорного органа, дата и длительность больничного конкретного работника относятся к специальным категориям данных по ст.9(1) GDPR. Хотя контролер провёл DPIA этого процесса и предоставил результаты регулятору для предварительной консультации, но регулятор посчитал, что контролер не смог продемонстрировать баланс своих законных интересов с интересами субъектов (LIA). И как следствие, меры снижения рисков были выбраны некорректно.

## Штраф за нарушение принципа «ограничения целью» (purpose limitation)

edpb  
European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS SEARCH

European Data Protection Board

News National News National News The Norwegian Data Protection Authority imposes a fine on the Municipality of Oslo, the Education Agency

### The Norwegian Data Protection Authority imposes a fine on the Municipality of Oslo, the Education Agency

Finley 23 October 2019

On October 11th, the Norwegian DPA also imposed an administrative fine of EUR 120 000 on the Municipality of Oslo, the Education Agency as a result of poor security of processing in a mobile app. The app is used for communication between school employees, parents and pupils. The fine was issued because the municipality had not implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The Municipality of Oslo did not appeal the decision.

The following were key elements in the Data Protection Authority's assessment:

1. One of the intended uses of the app is for parents to send messages regarding their children and absence from school using a free-text field. This enables communication of special category personal data, such as health data, regarding the children. There are no technical measures to prevent this from happening, and no information is given within the app that such transmission should be avoided. In line with data protection by design and default, alternative measures such as drop-down lists and tick boxes are more appropriate.
2. Poor app login security made it possible for unauthorised persons to access and alter personal data of more than 63 000 pupils in the first to tenth grade.
3. As a consequence of inadequate security testing before the app was launched, the app contained well-known security vulnerabilities.

Previously, the Data Protection Authority notified its intent to impose a fine of € 200 000 in response to the findings above. However, in the final amount was reduced to € 120 000 as there were mitigating factors present in the case. The municipality implemented measures to limit the damages as soon as it was made aware of the security flaws, and it has shown willingness to resolve the issues.

For further information, please contact the Norwegian SA: [international@datatilsynet.no](mailto:international@datatilsynet.no)

**Кто:** Datatilsynet (Норвегия)

**Кого:** Муниципалитет Осло, образовательное учреждение

**Когда:** 2019.10

**За что:** нарушение ст. 5, 25, 32 GDPR

**Как:** возможный штраф €120,000

**Причина:** недостаточная защита данных в приложении «Skolemelding», предназначенном для общения учителей, родителей и учащихся. Одно из назначений приложения - отправка сообщений в школу об отсутствии учащихся, в которых могут указываться сведения о состоянии их здоровья. При этом в приложении не было технических мер, препятствующих внесению и отправке таких сведений. Кроме того, слабая защита приложения привела к его взлому со стороны злоумышленников, которые смогли изменить данные 63,000 учащихся.



## Штраф за ненадлежащий механизм отзыва согласия на обработку персональных данных



The screenshot shows the EDPB website with the following content:

**edpb** European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

European Data Protection Board News National News National News Polish DPA: Withdrawal of consent shall not be impeded

### Polish DPA: Withdrawal of consent shall not be impeded

Wednesday 4 November 2019 PL

The President of the Personal Data Protection Office imposed an administrative fine of over PLN 201,000 for, inter alia, obstructing the exercise of the right to withdraw consent to the processing of personal data.

The company - ClickQuickNow Sp. z o.o. did not implement appropriate technical and organizational measures that would enable easy and effective withdrawal of consent to the processing of personal data and the exercise of the right to obtain the erasure of personal data (the "right to be forgotten"). Thus, it violated the principles of lawfulness, fairness and transparency of processing of personal data, specified in the GDPR.

The President of the Personal Data Protection Office (PDPO) found that the company's actions were also inconsistent with Article 7(3) of the GDPR. The company did not take into account the principle that withdrawal of consent should be as easy as giving consent - on the contrary, it applied complicated organisational and technical solutions with regard to the withdrawal of consent. Moreover, the company did not facilitate the exercise of the subject rights, as required by Article 12(2) of the GDPR.

The proceedings of the President of PDPO established that the company violated the abovementioned provisions of the GDPR, because the mechanism of the consent withdrawal, involving the use of a link included in the commercial information, did not result in a quick withdrawal. After the link was set up, messages addressed to the person interested in withdrawing consent were misleading. Moreover, the company forced stating the reason for withdrawing consent, which is not required by the law. Furthermore, failure to indicate the reason resulted in discontinuation of the process of withdrawing consent.

In his decision, the President of the PDPO also pointed out that the company processed, without any legal basis, the data of data subjects, who are not its customers and from whom the company received objections to processing their personal data. Thus, it also violated the so-called "right to be forgotten".

When determining the amount of the administrative fine, the President of the PDPO did not take into account any mitigating circumstances affecting the final penalty. He also decided that the company's action was intentional - providing contradictory communications to the data subject interested in withdrawing consent resulted in an ineffective withdrawal of consent. In this way, the company made it difficult, or even impossible, to exercise the rights of the data subjects.

The President of PDPO not only imposed an administrative fine on the company, but also ordered it to adjust the process of processing requests for withdrawing consent to data processing to the provisions of the GDPR. ClickQuickNow Sp. z o.o. has 14 days from the date of delivery of the decision to comply with the decision. The company must also delete the data of data subjects who are not its customers and objected to processing the personal data concerning them.

To read the press release in Polish, click [here](#)

The Polish text of the decision is available [here](#)

For further information, please contact the Polish DPA: [kanczstarja@uodo.gov.pl](mailto:kanczstarja@uodo.gov.pl)

**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** ClickQuickNow Sp. z o.o.

**Когда:** 2019.11

**За что:** нарушение ст. 5, 7(3), 12(2) GDPR

**Как:** штраф €47,000

**Причина:** не был обеспечен простой и эффективный механизм отзыва согласия субъекта (отзыв согласия должен быть таким же простым, как его предоставление) и реализации права на удаление данных, так как для отзыва согласия субъекту надо было перейти по ссылке и указать причину отзыва согласия, а без указания причины отзыв не выполнялся. Также компания продолжала обрабатывать персональные данные субъектов, отозвавших своих согласия и не являющихся клиентами компании, без правового основания.

## Штраф за неправомерное хранение и несоблюдение сроков хранения персональных данных



Berliner Beauftragte  
für Datenschutz  
und Informationsfreiheit

### Pressemitteilung

711.412.1

5. November 2019

#### Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft

Am 30. Oktober 2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) erlassen.

Bei Vor-Ort-Prüfungen im Juni 2017 und im März 2019 hat die Aufsichtsbehörde festgestellt, dass das Unternehmen für die Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendete, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen. Personenbezogene Daten von Mieterinnen und Mietern wurden gespeichert, ohne zu überprüfen, ob eine Speicherung zulässig oder überhaupt erforderlich ist. In begutachteten Einzelfällen konnten daher teilweise Jahre alte private Angaben betroffener Mieterinnen und Mieter eingesehen werden, ohne dass diese noch dem Zweck ihrer ursprünglichen Erhebung dienten. Es handelte sich dabei um Daten zu den persönlichen und finanziellen Verhältnissen der Mieterinnen und Mieter, wie z. B. Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Arbeitsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge.

Nachdem die Berliner Datenschutzbeauftragte im ersten Prüftermin 2017 die dringende Empfehlung ausgesprochen hatte, das Archivsystem umzustellen, konnte das Unternehmen auch im März 2019, mehr als eineinhalb Jahre nach dem ersten Prüftermin und neun Monate nach Anwendungsbeginn der Datenschutz-Grundverordnung weder eine Bereinigung ihres Datenbestandes noch rechtliche Gründe für die fortdauernde Speicherung vorweisen. Zwar hatte das Unternehmen Vorbereitungen zur Beseitigung der aufgefundenen Missstände getroffen. Diese Maßnahmen hatten jedoch nicht zur Herstellung eines rechtmäßigen Zustands bei der Speicherung personenbezogener Daten geführt. Die Verhängung eines Bußgeldes wegen eines

Pressesprecherin: Dalia Kues  
Geschäftsstelle: Cristina Vecchi  
E-Mail: [presse@datenschutz-berlin.de](mailto:presse@datenschutz-berlin.de)

Friedrichstr. 219 Tel: 030 13889 - 900  
10969 Berlin Fax: 030 2155050



**Кто:** Berliner Datenschutzbeauftragte (Германия)

**Кого:** Deutsche Wohnen SE (один из крупнейших наймодателей недвижимости в Германии)

**Когда:** 2019.11

**За что:** нарушение ст. 6 GDPR

**Как:** штраф €14,500,000

**Причина:** нарушение порядка хранения данных, так как из электронного архива компании невозможно было удалить данные. Персональные данные (финансовая информация, информация о социальном страховании) хранились без надлежащего правового основания.

## Штраф за нарушение законодательства о защите прав потребителей в Венгрии

The screenshot shows the website of the Hungarian Competition Authority (GVH). The main navigation bar includes 'HOME', 'FOR PROFESSIONAL USERS', and 'PRESS ROOM'. The 'PRESS ROOM' section is active, displaying a list of press releases on the left and the full text of a press release from 2019 on the right. The title of the press release is 'GVH imposed a fine of EUR 3.6 M on Facebook'. The text of the press release states that the GVH found that Facebook Ireland Ltd. had infringed competition law by advertising its services as being free of charge on its home page and Help Centre. The GVH imposed a fine of EUR 3.6 M on Facebook, which is the highest fine that the Authority has ever imposed in a consumer protection case. The press release also mentions that the GVH found that the slogans 'It's free and anyone can join' and 'Free and always will be' used by Facebook to attract users were deceptive and misleading.

**Кто:** Gazdasági Versenyhivatal – Агентство по вопросам конкуренции (Венгрия)

**Кого:** Facebook Ireland Ltd.

**Когда:** 2019.12

**За что:** нарушение Закона Венгрии о конкуренции

**Как:** штраф €3,600,000

**Причина:** Facebook Ireland Ltd. рекламировала свои сервисы как бесплатные («zero price»), хотя бизнес-модель Facebook заключается в привлечении пользователей контентом своей онлайн-платформы и сборе подробной информации об интересах своих пользователей, их поведении и покупательских привычках. Затем Facebook использует эти данные для продажи таргетированной рекламы. При этом сервисы Facebook фактически не являются бесплатными, так как пользователи косвенно оплачивают использование сервисов предоставлением своих персональных данных, при этом не до конца понимая все аспекты обработки своих данных и осознавая все сопутствующие этому риски.

## 756 Штраф за ненадлежащую процедуру идентификации



The image shows a screenshot of a website page from the German Federal Data Protection Commissioner (BfDI). The page header includes the BfDI logo and the text "Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit". Below the header is a navigation menu with "DATENSCHUTZ", "INFORMATIONSFREIHEIT", "INFOTHEK", "BFDI", and "ZENTRALE ANL". The breadcrumb trail reads "Infothek → Pressemitteilungen → BfDI verhängt Geldbußen gegen Telekommunikationsdie". The main heading is "BfDI verhängt Geldbußen gegen Telekommunikationsdienstleister". The sub-heading is "Bonn/Berlin, 9.12.2019". The text states that the BfDI has imposed a fine of 9,550,000 Euro on 1&1 Telecom GmbH for failing to implement sufficient technical and organizational measures to prevent unauthorized access to customer data. The text also mentions that the BfDI has imposed a fine of 10,000 Euro on Rapidata GmbH for similar reasons. A quote from Ulrich Kelber, the Federal Data Protection Commissioner, is included at the bottom of the screenshot.

**BfDI verhängt Geldbußen gegen Telekommunikationsdienstleister**

Bonn/Berlin, 9.12.2019

Ausgabe 30/2019  
Datum 09.12.2019

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat den Telekommunikationsdienstleister 1&1 Telecom GmbH mit einer Geldbuße in Höhe von 9.550.000 Euro belegt.

Das Unternehmen hatte keine hinreichenden technisch-organisatorischen Maßnahmen ergriffen, um zu verhindern, dass Unberechtigte bei der telefonischen Kundenbetreuung Auskünfte zu Kundendaten erhalten können. In einem weiteren Fall sprach der BfDI ein Bußgeld in Höhe von 10.000 Euro gegen die Rapidata GmbH aus.

Dazu sagte der Bundesbeauftragte Ulrich Kelber: "Datenschutz ist Grundrechtsschutz. Die ausgesprochenen Geldbußen sind ein klares Zeichen, dass wir diesen Grundrechtsschutz durchsetzen werden. Die europäische Datenschutzgrundverordnung (DSGVO) gibt uns die Möglichkeit, die unzureichende Sicherung von personenbezogenen Daten entscheidend zu ahnden. Wir wenden diese Befugnisse unter Berücksichtigung der gebotenen Angemessenheit an."

**Кто:** Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Германия)

**Кого:** 1&1 Telecom GmbH (провайдер телекоммуникационных услуг)

**Когда:** 2019.12

**За что:** нарушение ст. 32 GDPR

**Как:** штраф €9,550,000

**Причина:** любое лицо могло получить исчерпывающую информацию о данных любого абонента просто предоставив отделу обслуживания компании имя и дату рождения абонента. Такая процедура идентификации является ненадлежащим исполнением обязанности по применению соответствующих технических и организационных мер для защиты персональных данных. Благодаря сотрудничеству компании с надзорным органом наложенный штраф оказался близок к минимальному значению.

## 757 Штраф за ненадлежащее хранение 500,000 документов



The screenshot shows the ICO website header with the logo and tagline: "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." Navigation links include Home, Your data matters, For organisations, Make a complaint, and Action we've taken. The article title is "London pharmacy fined after 'careless' storage of patient data", dated 20 December 2019. The text states that Doorstep Dispensaree Ltd was fined £275,000 for failing to ensure the security of special category data. It details that 500,000 documents were left in unlocked containers, some of which were water-damaged. The documents contained personal information like names, addresses, dates of birth, NHS numbers, and medical information. The ICO investigation was launched after an alert from the Medicines and Healthcare Products Regulatory Agency.

**Кто:** Information Commissioner's Office (Великобритания)

**Кого:** Doorstep Dispensaree Ltd


**Когда:** 2019.12

**За что:** нарушение ст. 5 GDPR


**Как:** штраф €323,000

**Причина:** в открытых контейнерах на улице хранились 500,000 документов компании, содержащих такие категории персональных данных как имя, адрес, дата рождения, NHS-номер, медицинскую информацию, сведения о назначенных врачами рецептах. В итоге многие документы были сильно повреждены осадками. Расследование были начато ICO после получения информации от Агентства по регулированию лекарственных средств и товаров медицинского назначения (Medicines and Healthcare Products Regulatory Agency).

## Штраф за использование архива корпоративной электронной почты



Nemzeti Adatvédelmi és  
Információszabadság Hatóság



---

Ügyszám: NAIH/2019/51/11.  
(NAIH/2018/4986/H.)

Tárgy: Kérelmeknek helyt adó határozat

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) előtt [...] a továbbiakban: Kérelmező a [...] továbbiakban: Kötelezett által, személyes adatai jogellenes kezelése tényének megállapítására, személyes adatai törlésének elrendelésére, illetve személyes adatai jogellenes kezelésének megtiltására irányuló kérelmére indult adatvédelmi hatósági eljárásban az alábbi döntéseket hozza:

I. A Hatóság

**HATÁROZATÁBAN**

1) a Kérelmező

**kérelmének helyt ad**

és megállapítja, hogy a Kötelezett a korlátozott tárolhatóság elvét sértve tárolja a Kérelmező magánlevelezéseit, továbbá a tisztességes adatkezelés elvébe ütközően, megfelelő tájékoztatás nélkül, a célhoz kötött adatkezelés elvébe ütközően, megfelelő jogalap hiányában végzett dokumentumkeresést archivált e-mail-fiókjában.

2) A Hatóság megtiltja a Kötelezett számára, hogy tárolja a Kérelmező magánlevelezéseinek archivumát és utasítja a Kötelezettet arra, hogy a jelen határozat véglegessé válásától számított 15 napon belül a Kérelmező bevonásával és tájékoztatásával vizsgálja felül, hogy a Kérelmező archivált e-mail-fiókjai sérelmezett, Kötelezett általi tárolása és az azokban történő dokumentumkeresés során mely – a munkavégzéssel össze nem függő (magáncélu) – személyes adatait, levelezéseit ismerte meg, illetve tárolta, és azokat törölje azzal, hogy a jelen határozat megtámadására nyitva álló keresetindítási határidő lejártáig, illetve közigazgatási per indítása esetén a bíróság jogerős határozatáig a vitatott adatkezeléssel érintett adatok kezelését korlátozni kell oly módon, hogy azok nem törölhetők, illetve nem semmisíthetők meg, ugyanakkor a tároláson és a közigazgatási perben a bíróság általi felhasználáson kívül más módon nem használhatók fel. Ennek során a Kötelezett köteles lehetővé tenni, hogy a kizárólag magáncélu adatokról a Kérelmező saját céljára másolatot készítsen, továbbá köteles a nem törölt adatok vonatkozásában az adatkezelésről a Kérelmezőt megfelelően tájékoztatni.

3) A Hatóság hivatalból megállapítja, hogy a Kötelezett a Kérelmező archivált e-mail-fiókjában történő dokumentumkereséssel összefüggő adatkezelése során az elszámoltathatóság alapelvi követelményét megsérve nem tett megfelelő technikai, szervezési intézkedéseket, annak érdekében, hogy az általa, a munkavállalók számára biztosított e-mail-fiókok használatával, archiválásával összefüggésben biztosítsa a személyes adatok védelmét, és nem gondoskodott az érintettek megfelelő tájékoztatásáról, megsérve ezzel együtt az átláthatóság elvét is.

4) A Hatóság hivatalból utasítja a Kötelezettet arra, hogy a jelen határozat véglegessé válásától számított 30 napon belül megfelelő, a tisztességes adatkezelés alapelvi követelményével összhangban álló technikai, szervezési intézkedések megtételével gondoskodjon a munkavállalók számára biztosított e-mail-fiókok használatára, archiválására, illetve az archivált tartalmakban történő dokumentumkeresések során a személyes adatok védelméről, alkossa meg az ezekhez szükséges belső szabályokat és gondoskodjon az érintettek megfelelő tájékoztatásáról. Ennek keretében biztosítsa, hogy az e-mail-fiókok tárolására, archiválására, az archivált adatokban történő keresésre vonatkozó belső szabályozás, és az ezekre vonatkozó megfelelő tájékoztató megalkotásával tárolja, archiválja a munkavállalók e-mail-fiókjait és végezzen azokban dokumentumkeresést.

1125 Budapest,  
Szállagyi Erzsébet t. 22/C.

Tel.: +36 1 391-1400  
Fax: +36 1 391-1410

ugyfelszolgalat@naih.hu  
www.naih.hu

**Кто:** Nemzeti Adatvédelmi és Információszabadság Hatóság (Венгрия)

**Кого:** неизвестная компания

**Когда:** 2019.12

**За что:** нарушение ст. 5, 6 GDPR

**Как:** штраф €1,500

**Причина:** работодатель продолжал обработку и поиск писем в архиве корпоративной электронной почты работника, в которых содержалась личная переписка работника, после увольнения работника без правового основания. Работодатель не принял надлежащие организационные и технические меры для обеспечения безопасного для персональных данных поиска документов в архиве электронной почты, а также не проинформировал о таком процессе субъектов.

## Штраф за незаконный прямой маркетинг и навязывание контрактов на поставку продукции



### The Italian Supervisory Authority fines Eni Gas e Luce Eur 11.5 million. On account of unsolicited telemarketing and contracts

The Italian Supervisory Authority fines Eni Gas e Luce Eur 11.5 million  
On account of unsolicited telemarketing and contracts

The Italian Supervisory Authority imposed two fines on Eni Gas and Luce (Eg), totaling EUR 11.5 million, concerning respectively illicit processing of personal data in the context of promotional activities and the activation of unsolicited contracts. The fines were determined in the light of the parameters set out in the EU Regulation, including the wide range of stakeholders involved, the pervasiveness of the conduct, the duration of the infringement, and the economic conditions of Eg.

The **first fine of EUR 8.5 million** relates to unlawful processing in connection with telemarketing and teleselling activities as found during inspections and inquiries that were carried out by the Authority following several dozens of alerts and complaints received in the immediate aftermath of the full application of the GDPR.

The verifications revealed a limited number of cases, which however pointed to 'systematic' conduct by Eg and highlighted serious irregularities with regard to the general processing of data.

The violations brought to light include advertising calls made without the consent of the contacted person or despite that person's refusal to receive promotional calls, or without triggering the specific procedures for verifying the public opt-out register; the absence of technical and organisational measures to take account of the indications provided by users; longer than permitted data retention periods; and the acquisition of the data on prospective customers from entities (list providers) that had not obtained any consent for the disclosure of such data.

Having declared the conduct detected as unlawful, the Italian SA ordered Eg to put in place procedures and systems in order to verify, also by examining a large sample of customers, the consent of the persons included in the contact lists prior to the start of promotional campaigns. Eg will also have to ensure full automation of data flows from its database to the company's own black list, i.e., the list of those who do not wish to receive advertising.

The Italian SA further prohibited the company from using the data made available by the list providers if the latter had not obtained specific consent for the communication of such data to Eg.

The **second fine of EUR 3 million** concerns breaches due to the conclusion of unsolicited contracts for the supply of electricity and gas under 'free market' conditions. Many individuals complained to the Authority that they learned about the conclusion of a new contract only on receiving the letter of termination of the contract with the previous supplier or else the first Eg bills. In some cases, the complaints reported incorrect data in the contracts and forged signatures.

About 7200 consumers were affected by the above serious irregularities. The Authority's findings showed that the conduct of Eg in acquiring new customers through certain external agencies operating on its behalf led, in organisational and managerial terms, to processing activities in breach of the EU Regulation as they violated the principles of data fairness, accuracy and up-to-dateness.

Having established such unlawful conduct, the Italian SA ordered Eg to take several corrective measures and to introduce specific alerts in order to detect various procedural anomalies.

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Eni Gas e Luce

**Когда:** 2020.01

**За что:** нарушение ст. 5, 6 GDPR

**Как:** два штрафа общей суммой €11,500,000

**Причина:** первый штраф в размере €8,500,000 связан с незаконной обработкой персональных данных в рамках деятельности по телемаркетингу и телепродажам без учета отказов субъектов от получения рекламных сообщений. Было выявлено нарушение сроков хранения персональных данных, а также покупка данных о потенциальных клиентах от третьих лиц, не получивших согласие субъекта на раскрытие информации. Второй штраф в размере €3,000,000 касается нарушений в связи с заключением более 7,200 навязанных контрактов на поставку электроэнергии и газа в условиях «свободного рынка». Многие потребители жаловались, что они узнали о заключении нового контракта только после получения письма о расторжении контракта с предыдущим поставщиком или после получения первых счетов.

## Штраф за незаконный прямой маркетинг и нарушение принципа accountability



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Marketing: dal Garante privacy sanzione di 27 milioni e 800 mila euro a Tim

Marketing: dal Garante privacy [sanzione di 27 milioni e 800 mila euro a Tim](#)

Il Garante per la privacy [ha irrogato a Tim spa una sanzione di 27.802.946 euro](#) per numerosi trattamenti illeciti di dati legati all'attività di marketing. Le violazioni hanno interessato nel complesso alcuni milioni di persone.

Dal gennaio 2017 ai primi mesi del 2019, sono pervenute all'Autorità centinaia di segnalazioni relative, in particolare, alla ricezione di chiamate promozionali indesiderate effettuate senza consenso o nonostante l'iscrizione delle utenze telefoniche nel Registro pubblico delle opposizioni, oppure ancora malgrado il fatto che le persone contattate avessero espresso alla società la volontà di non ricevere telefonate promozionali. Irregolarità nel trattamento dei dati venivano lamentate anche nell'ambito dell'offerta di concorsi a premi e nella modulistica sottoposta agli utenti da Tim.

Dalla complessa attività istruttoria che ne è derivata, svolta anche con il contributo del Nucleo Speciale Tutela Privacy e Froid Tecnologiche della Guardia di Finanza, sono emerse numerose e gravi violazioni della disciplina in materia di protezione dei dati personali.

Tim ha dimostrato di non avere sufficiente contezza di fondamentali aspetti dei trattamenti di dati effettuati ([accountability](#)).

Tra i milioni di telefonate promozionali effettuate in sei mesi nei confronti di "non clienti" l'Autorità ha accertato che le società di call center incaricate da Tim hanno, in molti casi, contattato gli interessati senza il loro consenso. Una persona è stata chiamata 155 volte in un mese. In circa duecentomila casi, sono state contattate anche numerazioni "fuori lista", cioè non presenti negli elenchi delle persone contattabili di Tim. Sono state rilevate poi altre condotte illecite come l'assenza di controllo da parte della società sull'operato di alcuni call center; l'errata gestione e il mancato aggiornamento delle black list dove vengono registrate le persone che non vogliono ricevere pubblicità; l'acquisizione obbligata del consenso a fini promozionali per poter aderire al programma "Tim Party" con i suoi sconti e premi.

Nella gestione di alcune [app](#) destinate alla clientela, inoltre, sono state fornite informazioni non corrette e non trasparenti sul trattamento dei dati e sono state adottate modalità di acquisizione del consenso non valide. In alcuni casi è stata utilizzata modulistica cartacea con richiesta di un unico consenso per diverse finalità, inclusa quella di marketing.

La gestione dei [data breach](#) non è poi risultata efficiente, così come inadeguate sono risultate l'implementazione e la gestione da parte della Società dei sistemi che trattano dati personali (con violazione del principio di [privacy by design](#)). Disallineamenti sono emersi tra le black list di Tim e quelle dei call center incaricati, così come per le registrazioni audio dei contratti stipulati telefonicamente (verbal order). Le utenze di clienti di altri operatori, detenute da Tim in quanto gestore delle Reti, sono state conservate per un tempo superiore ai limiti di legge e inserite, senza il consenso degli interessati, in alcune campagne promozionali.

Oltre alla sanzione, l'Autorità ha imposto a Tim 20 misure correttive, tra divieti e prescrizioni. In particolare, ha vietato a Tim l'uso dei dati a fini di marketing di chi aveva espresso ai call center il proprio diniego a ricevere telefonate promozionali, dei soggetti presenti in black list e dei "non clienti" che non avevano dato il consenso.

La società non potrà più utilizzare neanche i dati della clientela raccolti mediante le app "My Tim", "Tim Persona" e "Tim Smart Kid" per finalità diverse dall'erogazione dei servizi senza un consenso libero e specifico.

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** TIM S.p.A.

**Когда:** 2020.02

**За что:** нарушение ст. 5, 6 GDPR

**Как:** штраф €27,802,946 и 20 корректирующих мер

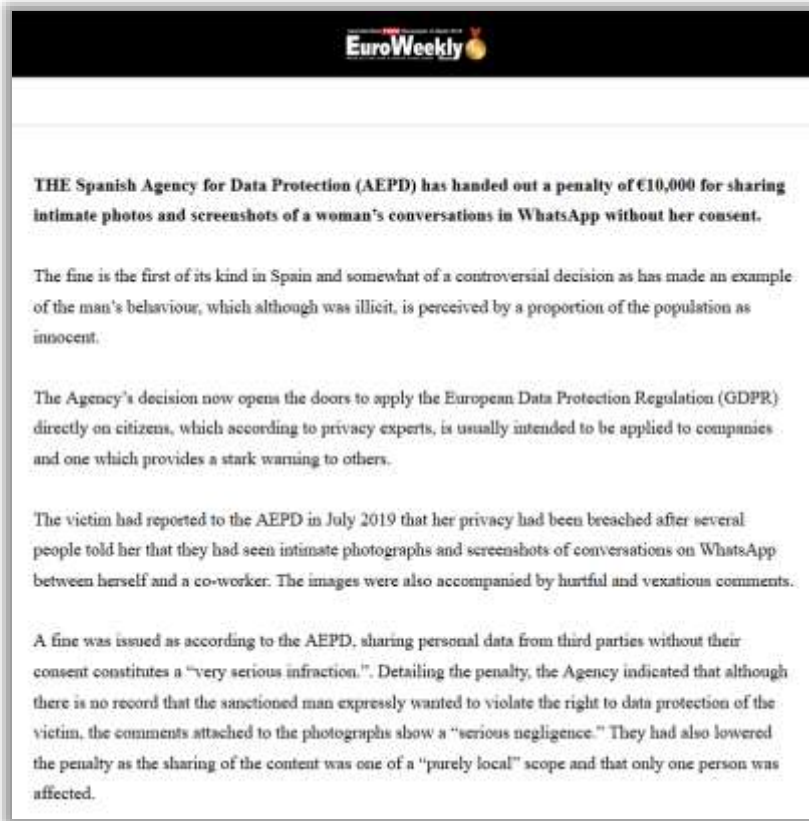
**Причина:** контролер совершал рекламные звонки без согласия субъектов (субъекты были указаны в Public Register do-not-call list или ранее отказались от получения таких звонков). Данное нарушение затронуло несколько миллионов субъектов. Так, одному человеку позвонили 155 раз за месяц.

Также контролер не продемонстрировал исполнение принципа accountability. Кроме того, надзорный при проверке выявил, что согласия на маркетинг, если и собирались с субъектов, то были обязательными для присоединения к программе Tim Party, предусматривающей получение скидок и призов. Информация об обработке персональных данных предоставлялась субъектам неполной и неточной (в приложениях).

**2023.04** на компанию был наложен [повторный штраф](#) €7,631,175 за незаконные практики телемаркетинга.



## Штраф физическому лицу за незаконный обмен интимными фото и копиями переписки



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** физическое лицо

**Когда:** 2020.02

**За что:** нарушение ст. 5, 6 GDPR

**Как:** штраф €10,000

**Причина:** обмен интимными фото и копиями переписки женщины в WhatsApp без ее согласия. По заявлению потерпевшей, ее личная жизнь была нарушена после распространения таких данных о ней в сети.

## 762 Штраф за необоснованное полагание на законный интерес

 **AUTORITEIT  
PERSOONSGEGEVENS**

Autoriteit Persoonsgegevens  
Postbus 93374, 2509 AJ Den Haag  
Bezuidenhoutseweg 30, 2594 AV Den Haag  
T 070 8888 500 - F 070 8888 501  
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Per loerier  
KNLTB  
[VERTROUWELIJK]  
Displayweg 4  
3821 BT AMERSFOORT

Datum  
20 december 2019

Ons kenmerk  
[VERTROUWELIJK]

Contactpersoon  
[VERTROUWELIJK]  
070 8888 500

Onderwerp  
Besluit tot het opleggen van een bestuurlijke boete

Geachte [VERTROUWELIJK],

De Autoriteit Persoonsgegevens (AP) heeft besloten aan de vereniging Koninklijke Nederlandse Lawn Tennisbond (KNLTB) een bestuurlijke boete van € 525.000,- op te leggen, omdat de KNLTB in juni en juli 2018 ten behoeve van het genereren van inkomsten een bestand met persoonsgegevens van zijn leden heeft verstrekt aan twee sponsors ten behoeve van direct marketingactiviteiten van deze sponsors. Voor zover het de verstrekking en het gebruik betreft van persoonsgegevens van leden die vóór 2007 lid zijn geworden van de KNLTB, geldt dat dit een onverenigbare verdere verwerking is. Daarmee heeft de KNLTB artikel 5, eerste lid, aanhef en onder b, van de AVG overtreden. Voor zover het de verstrekking en gebruik betreft van persoonsgegevens van leden die ná 2007 lid geworden van de KNLTB, geldt dat daarvoor geen rechtmatige grondslag bestond. Daarmee heeft de KNLTB artikel 5, eerste lid, aanhef en onder a), artikel 6, eerste lid, van de AVG overtreden.

Hierna wordt het besluit nader toegelicht. Hoofdstuk 1 betreft een inleiding en hoofdstuk 2 beschrijft het wettelijk kader. In hoofdstuk 3 worden de belangrijkste feiten in deze zaak op een rij gezet. In hoofdstuk 4 beoordeelt de AP de feiten op grond van het wettelijk kader en wordt geconcludeerd dat de KNLTB de AVG heeft overtreden. In hoofdstuk 5 wordt de hoogte van de bestuurlijke boete gemotiveerd. Tenslotte bevat hoofdstuk 6 het dictum en de rechtsmiddelenclausule.

**Who:** Autoriteit Persoonsgegevens (Нидерланды)

**Who:** Теннисная ассоциация KNLTB

**When:** 2020.03

**For what:** нарушение ст. 5, 6 GDPR

**How:** штраф €525,000

**Reason:** контролер передал контактные данные нескольких тысяч участников ассоциации спонсорам, которые потом установили прямой контакт с субъектами. Контролер считал, что передаёт данные на основании своего законного интереса.

## Штраф за безальтернативную биометрическую идентификацию в школе

Urząd Ochrony Danych Osobowych

Wpisz frazę której szukasz

Infolinia Urzędu 606-950-000

Prezes i Urząd    Prawo    Edukacja    Współpraca

+ Aktualności

### Szkoła z karą za odciski palca uczniów

Prezes Urzędu Ochrony Danych Osobowych nałożył karę w wysokości 20 tys. zł w związku z naruszeniem polegającym na przetwarzaniu danych biometrycznych dzieci podczas korzystania przez nie ze szkolnej stołówki.

Szkoła przetwarzała dane szczególnych kategorii (dane biometryczne) 680 dzieci bez podstawy prawnej, mogąc jednocześnie zastosować inne formy identyfikacji uczniów.

Za to naruszenie została nałożona administracyjna kara pieniężna na Szkołę Podstawową nr 2 z Gelańska. Ponadto Prezes UODO nakazał jej usunięcie danych osobowych przetworzonych do postaci cyfrowej informacji o charakterystycznych punktach linii papilarnych palców dzieci oraz zaprzestanie dalszego zbierania danych osobowych.

Prezes UODO po przeprowadzeniu z urzędu postępowania administracyjnego ustalił, że szkoła korzysta z czytnika biometrycznego przy wejściu do stołówki szkolnej, który identyfikuje dzieci w celu weryfikacji uiszczenia opłaty za posiłek.

Postępowanie wykazało, że szkoła pozyskuje te dane i przetwarza je na podstawie pisemnej zgody rodziców lub opiekunów prawnych. Stosowane rozwiązanie funkcjonuje od 1 kwietnia 2015 r. W obecnym w roku szkolnym 2019/2020 z czytnika biometrycznego korzysta 680 uczniów, a czterech uczniów z alternatywnego systemu identyfikacji.

W tej sprawie trzeba podkreślić, że przetwarzanie danych biometrycznych nie jest niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnień dziecka do odebrania obiadu. Szkoła może przeprowadzić identyfikację za pomocą innych środków, które nie ingerują tak dalece w prywatność dziecka. Ponadto szkoła umożliwiała korzystanie z usług stołówki szkolnej nie tylko za pomocą odcisku linii papilarnych, ale i karty elektronicznej lub na podstawie nazwiska i numeru umowy. Zatem, w Szkole istnieją alternatywne formy identyfikacji uprawnień dziecka do odebrania obiadu.



**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** школа

**Когда:** 2020.03

**За что:** нарушение ст. 5, 9 GDPR

**Как:** штраф €4,400

**Причина:** контролер обрабатывал биометрические данные (отпечатки пальцев) школьников без правового основания в целях идентификации в школьной столовой в для проверки оплаты за питание. Обработка происходила на основании письменного согласия законных представителей детей. При этом предусмотренные в школе альтернативные меры идентификации не предоставляли субъектам равноценных возможностей.

## Штраф за нарушение Google права субъекта на забвение (right to be forgotten)



The screenshot shows the website of the Swedish Datainspektionen (Data Protection Authority). The header includes the logo, navigation links (OM OSS, KONTAKTA OSS, PRESS, A-Ö, IN ENGLISH), and a search bar. A red navigation bar contains categories: AKTUELLT, VÄGLEDNINGAR, LAGAR OCH REGLER, and UTBILDNINGAR OCH KONFERENSER. The main content area features a breadcrumb trail: Start → Nyheter → Datainspektionen utfärdar sanktionsavgift mot Google, dated 2020-03-11. The article title is 'Datainspektionen utfärdar sanktionsavgift mot Google'. The text describes a fine of 75 million kronor imposed on Google for violating GDPR, specifically for not deleting search results containing personal data upon request. It mentions a 2017 investigation and a 2018 investigation that led to the fine. A quote from Lena Lindgren Schelin, the general director, is also included.

**Start** → **Nyheter** → **Datainspektionen utfärdar sanktionsavgift mot Google**

Publicerad 2020-03-11

### Datainspektionen utfärdar sanktionsavgift mot Google

*Datainspektionen utfärdar en sanktionsavgift på 75 miljoner kronor mot Google för att företaget bryter mot GDPR. Orsaken är att Google brister i sitt sätt att hantera rätten att få sökresultat borttagna.*

2017 blev Datainspektionen klar med en granskning av hur Google hanterar rätten för enskilda att få sökresultat borttagna från Googles sökmotor för sökningar som innehåller personens namn i fall då resultaten exempelvis är oriktiga, irrelevanta eller överflödiga. Datainspektionen förelade då Google att ta bort ett antal sökträffar.

2018 inledde Datainspektionen en ny granskning av Google efter att ha fått indikationer på att flera av de resultat som skulle ha tagits bort fortfarande visades i sökningar. Nu är myndigheten klar med denna granskning och utfärdar en sanktionsavgift mot Google.

– Dataskyddsförordningen, GDPR, ökar kraven på organisationer som samlar in och hanterar personuppgifter och stärker enskildas rättigheter. En viktig sådan rättighet är möjligheten för enskilda att få sökresultat borttagna. Nu ser vi att Google brister i sitt sätt att hantera denna rättighet, säger Lena Lindgren Schelin, generaldirektör för Datainspektionen.

**Кто:** Datainspektionen (Швеция)

**Кого:** Google

**Когда:** 2020.03

**За что:** нарушение ст. 17 GDPR

**Как:** штраф €7,000,000

**Причина:** Google как оператор поисковой системы не выполнил свои обязательства в отношении права на исключение результатов поисковой выдачи, содержащих персональные данные. В одном из случаев Google слишком узко интерпретировал запрос субъекта и не удалил все требуемые веб-адреса. Во втором случае Google отреагировал на запрос субъекта с неоправданной задержкой.

Была выявлена недобросовестная практика, по которой Google уведомляет владельцев веб-сайтов о том, какие ссылки на их ресурсы были исключены из поисковой выдачи и кто стоял за запросом об их исключении. Это позволяет владельцам сайтов повторно опубликовать исключенную информацию на других страницах, которые затем опять попадают в поисковую выдачу Google.



**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** Vis Consulting Sp. z o.o.

**Когда:** 2020.04

**За что:** нарушение ст. 31, 58(1)(e) и (f) GDPR

**Как:** штраф €4,400 и возможная уголовная ответственность руководителя контролера

**Причина:** контролер воспрепятствовал проведению проверки со стороны национального регулятора, который решил проверить Vis Consulting по итогам проверки их клиента, которому оказывались услуги аутсорсинга телемаркетинга. Но инспекторы после предварительного уведомления о проверке не нашли никого по адресу контролера. Ещё дважды регулятор безуспешно пытался выйти на контакт с контролером. Владельцы этой компании решили ее ликвидировать. В соответствии с GDPR такое поведение может повлечь за собой штраф, ограничение личной свободы или тюремное заключение на срок до двух лет. Регулятор уведомил районную прокуратуру в Катовице, которая направила в суд обвинительное заключение против руководителя Vis Consulting.

## Штраф за использование биометрической системы учета рабочего времени



**AUTORITEIT  
PERSOONSgegevens**

Home Corona Over privacy ▾ Onderwerpen ▾ Zelf doen ▾

# Boete voor bedrijf voor verwerken vingerafdrukken werknemers

Nieuwsbericht / 30 april 2020 Categorie: [Biometrie, Controle van werknemers](#)

Werknemers van een bedrijf hebben hun vingerafdrukken moeten laten scannen voor aanwezigheids- en tijdsregistratie. De Autoriteit Persoonsgegevens (AP) heeft na onderzoek geconcludeerd dat het bedrijf geen vingerafdrukken van medewerkers had mogen verwerken. Het bedrijf kan zich namelijk niet beroepen op een uitzonderingsgrond voor het verwerken van bijzondere persoonsgegevens. Het bedrijf krijgt hiervoor een boete van 725.000 euro.

**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** неназванная компания

**Когда:** 2020.04

**За что:** нарушение ст. 5 и 6 GDPR

**Как:** штраф €725,000

**Причина:** компания осуществляла сканирование отпечатков пальцев своих работников в рамках использования биометрической системы учета рабочего времени. Согласно позиции надзорного органа, использование систем биометрической идентификации возможно только в случае, если субъекты данных предоставляют явное согласие или если использование биометрических данных необходимо для целей аутентификации и обеспечения безопасности. Особо было отмечено, что работники зависят от своего работодателя, поэтому их согласие на использование подобной системы не может быть оценено как свободное.

## Штраф за отсутствие процедуры по публикации персональных данных на веб-сайте

The screenshot shows the website of Datainspektionen. At the top, there is a logo and navigation links: OM OSS, KONTAKTA OSS, PRESS, A-Ö, IN ENGLISH. Below this is a search bar with the text "Sök frågor och svar, vägledning och regler...". A red navigation bar contains the following categories: AKTUELLT, VÄGLEDNINGAR, LAGAR OCH REGLER, and UTBILDNINGAR OCH KONFERENSER. The article title is "Fel publicera känsliga personuppgifter på Region Örebro läns webb". The date is "Publicerad 2020-05-12". The breadcrumb trail is "Start → Nyheter → Fel publicera känsliga personuppgifter på Region Örebro läns webb".

**Fel publicera känsliga personuppgifter på Region Örebro läns webb**

*Datainspektionens granskning visar att Hälso- och sjukvårdsnämnden i Region Örebro län gjort fel vid publicering av känsliga personuppgifter på regionens webbplats om en patient som är intagen på rättspsykiatrisk klinik.*

Datainspektionen har tagit emot ett klagomål mot Hälso- och sjukvårdsnämnden i Region Örebro län som gjorde gällande att känsliga personuppgifter om en patient som är intagen på rättspsykiatrisk klinik publicerats på regionens webbplats.

– Vår granskning av det inträffade visar att känsliga personuppgifter felaktigt publicerats och har legat öppna på regionens webbplats, säger Elin Hallström, jurist på Datainspektionen.

Av Datainspektionens granskning framgår att det inte finns några skriftliga rutiner som rör publicering av handlingar och personuppgifter på webbplatsen. Rutiner kring publiceringen delges muntligt. I detta fall har de muntliga rutinerna inte följts och handlingen publicerades av misstag, vilket tyder på att nämnden inte har vidtagit tillräckliga organisatoriska åtgärder för att säkerställa att personuppgifter skyddas från att felaktigt publiceras på regionens webbplats.

**Кто:** Datainspektionen (Швеция)

**Кого:** Департамент здравоохранения в регионе Эребруа (Hälso- och sjukvårdsnämnden i Region Örebro län)

**Когда:** 2020.05

**За что:** нарушение ст. 5 и 6 GDPR

**Как:** штраф €11,200

**Причина:** публикация на веб-сайте специальных категорий данных - информации о госпитализации пациентов в судебно-психиатрической клинике (по ошибке). Регулятор при проверке отметил, что у контролера не разработаны документированные процедуры по публикации информации (включая персональные данные) на веб-сайте. Также отсутствовали цель обработки и правовое основание.

## 768 Штраф за нарушение права субъекта на доступ к данным



**DATATILSYNET**

Du er her: Forside / Presse og nyheder / Nyhedsarkiv / 2020 / maj / JobTeam ind

### JobTeam indstillet til bøde

Publiceret 15-05-2020

Nyhed

Datatilsynet vurderer, at JobTeam i forbindelse med en sag om retten til indsigt ikke har levet op til de grundlæggende krav i databeskyttelsesforordningen (GDPR) om, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde.



**Кто:** Datatilsynet (Дания)

**Кого:** JobTeam

**Когда:** 2020.05

**За что:** нарушение ст. 5 и 15 GDPR

**Как:** штраф €6,500

**Причина:** компания уничтожила данные субъекта в ответ на запрос о предоставлении доступа к данным, таким образом, запрос субъекта не был выполнен. По мнению датского регулятора, это является грубым нарушением фундаментальных прав субъекта.



## Штраф за нарушение права субъекта на получение исчерпывающей информации об обработке данных

The screenshot shows the website of the Office of the Data Protection Ombudsman's sanctions board (Tietosuojavaltuutetun toimisto). The page is in Finnish, with a search bar at the top right and a navigation menu. The main article is titled "Office of the Data Protection Ombudsman's sanctions board imposed three administrative fines for data protection violations" and is dated 22.5.2020. The article text mentions that the board imposed administrative fines on three companies for violations of data protection legislation on 18 May, concerning insufficient information on data protection rights, neglecting to conduct a data protection impact assessment, and the unnecessary collection of personal data.

**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

**Кого:** Posti Oy (Почта Финляндии)

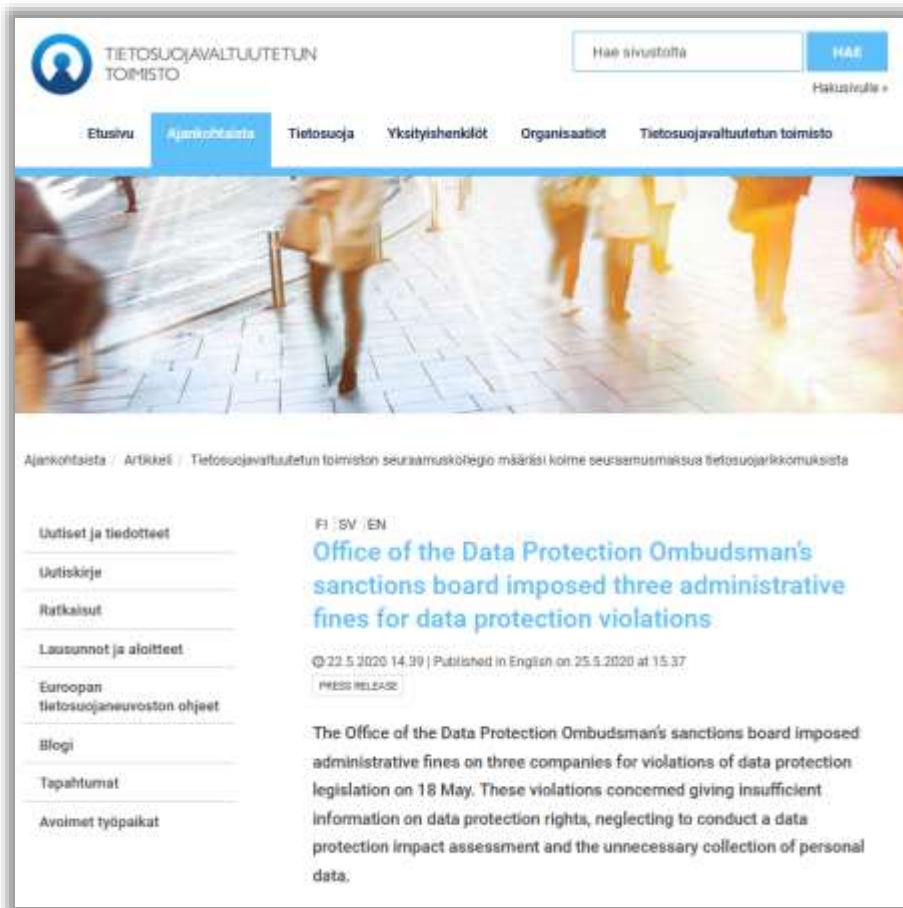
**Когда:** 2020.05

**За что:** нарушение ст. 5, 12 и 21 GDPR

**Как:** штраф €100,000

**Причина:** 161,000 субъектов получили письма и рекламу от разных компаний после того, как уведомили Почту о смене адреса. По результатам проверки регулятор обнаружил, что компания не уведомила субъектов об их правах, в том числе о праве на возражение против раскрытия данных, в связи с внесением уведомлений об изменении адреса. Компания уведомила только клиентов, которые приобрели дополнительные услуги в дополнение к смене адреса.

## Штраф за отслеживание местоположения работников без проведения DPIA



**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

**Кого:** Kymen Vesi Oy

**Когда:** 2020.05

**За что:** нарушение ст.35 GDPR

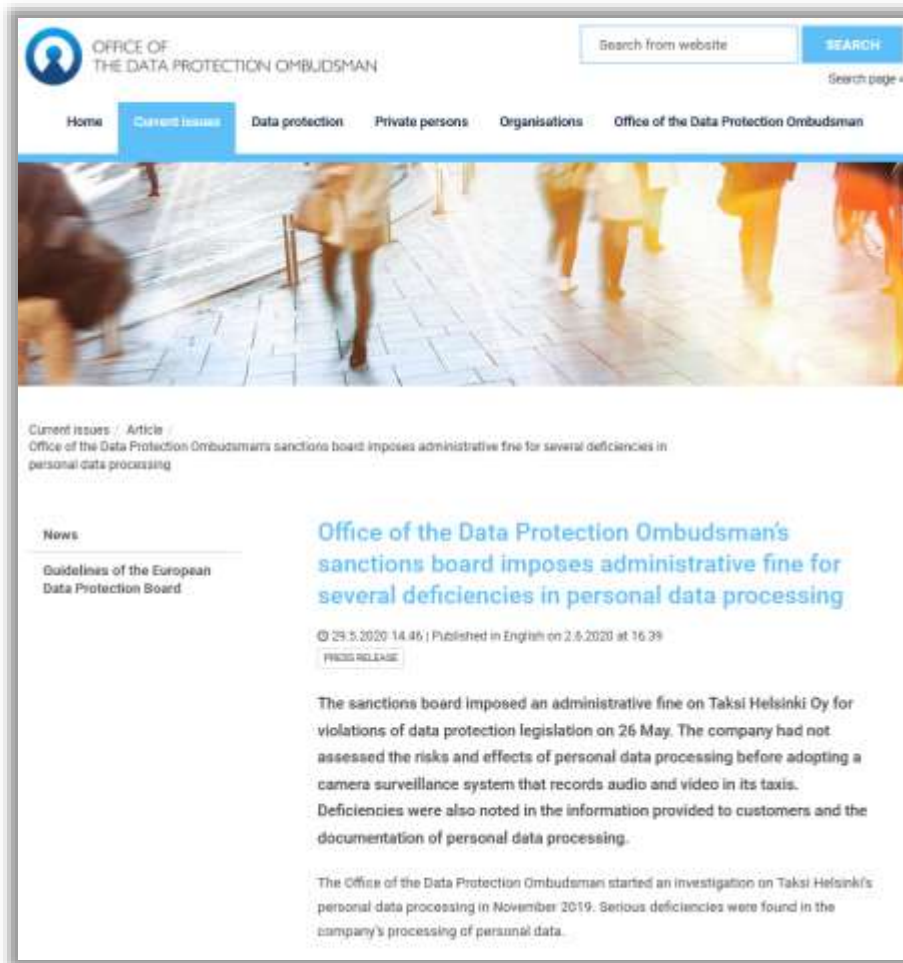
**Как:** штраф €16,000

**Причина:** компания обрабатывала данные о местоположении работников путём отслеживания транспортных средств с использованием специализированной системы. Контролер не провёл DPIA перед началом обработки данных. Данные о местоположении использовались в том числе для мониторинга отработанных часов.

Было указано, что DPIA для данного процесса необходим, т.к. процесс относится к высокорискованным:

- обрабатываются данные уязвимых субъектов (работников);
- обрабатываются данные о местоположении в целях осуществления систематического мониторинга.

## Штраф за внедрением системы видеонаблюдения в такси без проведения DPIA



**Кто:** TietosuojaValtuutetun toimisto (Финляндия)

**Кого:** Taksi Helsinki Oy

**Когда:** 2020.05

**За что:** нарушение ст. 5, 6, 35 GDPR

**Как:** штраф €72,000

**Причина:** компания не оценила риски обработки данных, необходимость такой обработки и влияние обработки на субъектов (DPIA) перед внедрением системы видеонаблюдения, записывающей аудио и видео в такси. Также были обнаружены недостатки в информации, предоставляемой клиентам (субъекты не были уведомлены об аудиозаписи), и документации, регламентирующей обработку персональных данных (в Privacy Notice отсутствовала информация о принятии решений исключительно по результатам автоматической обработки и профилировании, некорректно определены роли).

Кроме того, аудиозаписи обрабатывались по ошибке и без необходимости: избыточный сбор и отсутствие правового основания.

## Штраф за неправомерную обработку персональных данных в рамках функции «пригласи друга»



**Кто:** l'Autorité de protection des données (Бельгия)

**Кого:** провайдер неназванной социальной сети

**Когда:** 2020.05



**За что:** нарушение ст. 5 и 6 GDPR

**Как:** штраф €50,000

**Причина:** незаконная обработка данных в рамках функции «пригласи друга», реализованной на социальной платформе. Провайдер собирал и хранил данные контактов участников социальной сети с целью отправки приглашений для присоединения к платформе на основании согласия самих участников. Также провайдер собирал с участников согласия на обработку данных их контактов с использованием предустановленных галочек в поле согласие, что регулятор счёл незаконным.

Бельгийский регулятор использовал «one-stop-shop» механизм, был ведущим контролирующим органом и взаимодействовал по этому случаю ещё с 23 регуляторами из 16 стран ЕС.

# Штраф за предоставление некорректной информации об обработке файлов cookie



1/6

• Procedimiento Nº: PS/00299/2019  
938-051119

**RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR**

En el procedimiento sancionador PS/00299/2019, instruido por la Agencia Española de Protección de Datos, a la entidad TWITTER INTERNATIONAL COMPANY (TWITTER SPAIN, S.L.), con CIF. B86672318, titular de la página web: [www.twitter.com](http://www.twitter.com), (en adelante "la entidad reclamada"), por presunta infracción a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), y en base a los siguientes:

**ANTECEDENTES**

**PRIMERO:** con fecha 04/05/18, D. A.A.A., (en adelante, "el reclamante"), presentó escrito ante la Agencia Española de Protección de Datos, en la que, entre otras, denunciaba:

*"La red Twitter facilita información inadecuada sobre las cookies que utiliza, lo que afecta a usuarios y no usuarios de la red social. Twitter no identifica con claridad todos los usos y socios de Twitter que podrían utilizar esta información de las cookies. También existen cookies que se cargan directamente, sin acción alguna por parte de la persona que accede a la página inicial".*

**SEGUNDO:** Con fecha 04/10/18 y 13/06/19, por los Servicios de Inspección de la Agencia Española de Protección de datos, se practican diligencias de investigación, teniendo conocimiento de lo siguiente:

a).- Al acceder al sitio web [www.twitter.com](http://www.twitter.com), (página de bienvenida), y sin haber realizado ningún tipo de acción, se comprueba que se almacenan automáticamente en el navegador, las siguientes cookies:

cookie	permanente	Uso
_ga	2 años	Está asociado con Google Universal Analytics, que es una actualización importante del servicio de análisis más comúnmente utilizado por Google. Esta cookie se usa para distinguir usuarios únicos al asignar un número generado aleatoriamente como un identificador de cliente. Se incluye en cada solicitud de página en un sitio y se utiliza para calcular los datos de visitantes, sesiones y campañas para los informes de análisis de sitios... El propósito principal de esta cookie es: Rendimiento.
_gat	1 minuto	Este nombre de cookie está asociado con Google Universal Analytics, de acuerdo con la documentación que se utiliza para regular la tasa de solicitud, lo que limita la recopilación de datos en sitios de alto tráfico. Caduca a los 10 minutos. El propósito principal de esta cookie es: Rendimiento.
_gid	1 día	Este nombre de cookie está asociado con Google Universal Analytics. Esto parece ser una nueva cookie y desde la primavera de 2017 no hay información disponible de Google. Parece almacenar y actualizar un valor único para cada página visitada. El propósito principal de esta cookie es: Rendimiento.
_twitter_sess	Caduca al finalizar la sesión	Esta cookie permite que los visitantes del sitio web utilicen las funciones relacionadas con Twitter desde la página que visitan. El propósito principal de esta cookie es: Funcionalidad.
Cif0	6 horas	Aún no hay información general sobre esta cookie basada únicamente en su nombre. El propósito principal de esta cookie es: Desconocido.

C/ Jorge Juan, 6  
28001 - Madrid

www.aepd.es  
sedesapgd.gob.es

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Twitter Spain S.L.

**Когда:** 2020.06

**За что:** нарушение ст. 22 Закона об услугах информационного общества и электронной коммерции (LSSI)

**Как:** штраф €30,000

**Причина:** контролер предоставлял некорректную информацию об обработке файлов cookie, что оказало негативное влияние на пользователей ресурса. Так, Twitter явно не определил всех пользователей и партнёров компании, которые могли использовать куки. Также некоторые куки загружались без дополнительных действий со стороны пользователя (на главной странице) и автоматически сохранялись в браузере. Через всплывающее уведомление (баннер о куки) не было предусмотрено внесение изменений в порядок обработки куки, например, отказаться от такой обработки.

## 774 Штраф за нарушение права субъекта на доступ к данным



The screenshot shows the website of the Autoriteit Persoonsgegevens (AP). The header includes the AP logo, the text 'AUTORITEIT PERSOONSgegevens', and navigation links: 'Home', 'Corona', 'Over privacy', 'Onderwerpen', and 'Zelf doen'. The main content area features a large headline: 'Boete voor BKR vanwege kosten bij inzage persoonsgegevens'. Below the headline, it indicates the article is a 'Nieuwsbericht / 6 juli 2020' and lists categories: 'Recht op inzage', 'Rechten van betrokkenen', and 'Krediet, inkomen en faillissement'. The article text states that the Stichting Bureau Krediet Registratie (BKR) is fined for imposing unnecessary barriers to access personal data, and that the AP has imposed a fine of 830,000 euros.

**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** Бюро кредитных историй (Stichting Bureau Krediet Registratie)

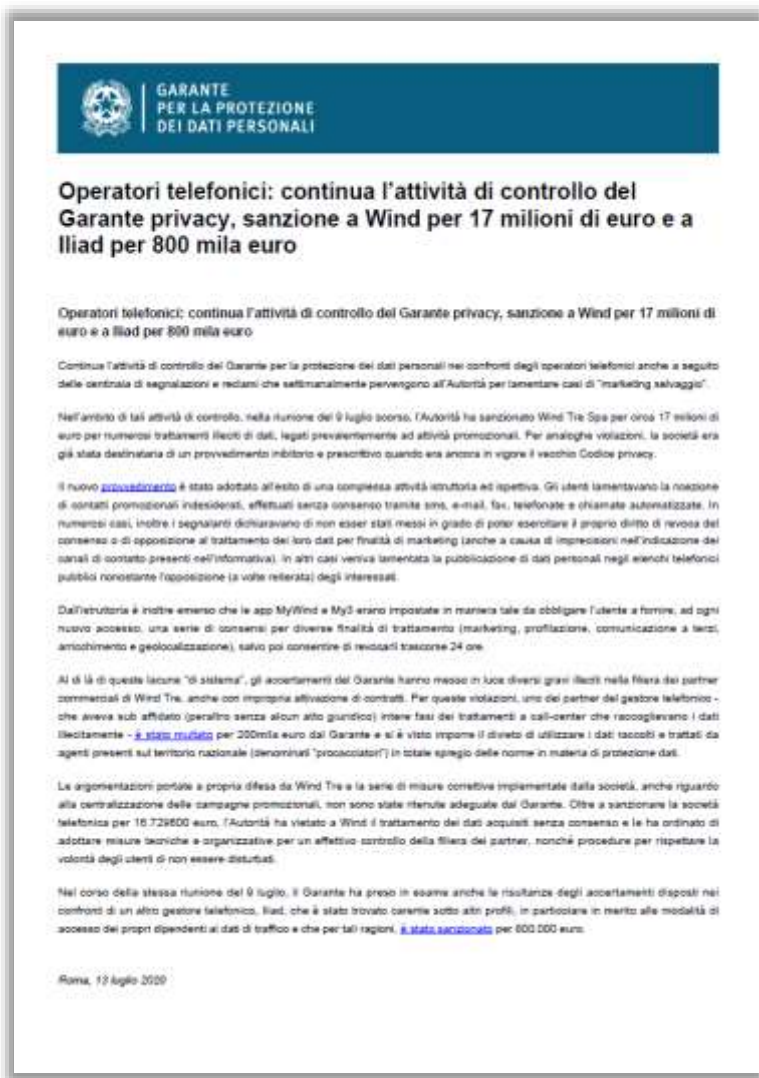
**Когда:** 2020.07

**За что:** нарушение ст. 12(2), 15 GDPR

**Как:** штраф €830,000

**Причина:** Бюро предлагало субъектам возможность бесплатного ознакомления с кредитной историей не чаще одного раза в год и только в письменной форме (с получением по почте). Альтернативный способ - получать доступ к своим данным в электронной форме за отдельную плату без ограничения количества ознакомлений. Бюро с назначенным штрафом не согласилось и обжаловало его в суде.

## Штраф за незаконный прямой маркетинг и отсутствие контроля над обработкой данных партнерами



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Wind Tre S.p.A.

**Когда:** 2020.07

**За что:** нарушение ст. 5(1) и (2), 6(1)(a), 12, 24 и 25 GDPR

**Как:** штраф €16,729,600, запрет на обработку данных и предписание эффективно контролировать партнеров

**Причина:** на действия компании подали жалобы сотни заявителей - субъектов данных. Wind Tre были вменены следующие нарушения:

1. множество фактов получения заявителями маркетинговых коммуникаций посредством SMS, электронной почты, телефонных звонков без предварительного согласия субъектов;
2. отдельные заявители не смогли реализовать свое право на отзыв согласия и на возражение против обработки данных в целях прямого маркетинга, поскольку контактная информация, содержащаяся в политике конфиденциальности Wind Tre, была неполной;
3. данные заявителей были опубликованы в открытых телефонных списках, несмотря на их возражение;
4. мобильные приложения «MyWind» и «My3» были настроены таким образом, чтобы обязывать пользователя предоставлять свое согласие на обработку персональных данных при каждом доступе к функционалу предложения, оставляя возможность отозвать согласие только через 24 часа;
5. были замечены различные недостатки в управлении Wind Tre своими сторонними партнерами - обработчиками данных.



**Кто:** l'Autorité de protection des données (Бельгия)

**Кого:** Google Belgium SA

**Когда:** 2020.07

**За что:** нарушение ст. 6(1)(f), 12(1)(4) и 17(1)(a) GDPR

**Как:** штраф €600,000 и предписание внести изменения в веб-форму в течение 2 месяцев

**Причина:** Google Belgium SA отклонил запрос граждан Бельгии об удалении из поисковой выдачи Google ссылок на материалы в СМИ, которые могут нанести серьезный ущерб их репутации (в материалах шла речь недоказанных фактах домогательств). При этом DPA согласился с тем, что сведения об отношениях граждан к определенным политическим партиям, учитывая их публичную роль, представляют общественный интерес и могут не удаляться из свободного доступа.

Кроме того, надзорный орган указал на недостаточно явное указание в соответствующей веб-форме Google (созданной для реализации права на забвение) на роли компаний Google в качестве контролеров данных для различных целей. Несмотря на утверждение Google о том, что жалоба граждан не может быть удовлетворена, поскольку она была подана против Google Belgium SA, а контролером данных является Google LLC, деятельность Google Belgium и Google LLC неразрывно связаны, поэтому Google Belgium может нести солидарную ответственность.



## 777 Штраф за неудаление данных 500,000 клиентов



**DATATILSYNET**

Du er her: [Forside](#) / [Presse og nyheder](#) / [Nyhedsarkiv](#) / [2020](#) / [jul](#) / [Arp-Hansen Hotel Group A/S](#)

### Arp-Hansen Hotel Group A/S indstilles til bøde

Publiceret 28-07-2020

Nyhed

Datatilsynet politianmelder Arp-Hansen og indstiller virksomheden til en bøde på 1.100.000 kr. for manglende sletning af ca. 500.000 kundeprofiler.



**Кто:** Datatilsynet (Дания)

**Кого:** Arp-Hansen Hotel Group A/S

**Когда:** 2020.07

**За что:** нарушение ст. 5(1)(e) GDPR

**Как:** штраф €147,800 и сообщение в полицию

**Причина:** что в ходе проверки ИТ-систем контролера было обнаружено, что система бронирования содержала много персональных данных (профилей клиентов), которые должны были быть удалены в соответствии с установленными самим контролером сроками хранения данных несколькими годами ранее.

## Штраф за нарушение принципа минимизации данных и за избыточное хранение данных 28 миллионов субъектов

**CNIL.**

*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

### **SPARTOO : sanction de 250 000 euros et injonction sous astreinte de se conformer au RGPD**

05 août 2020

*La CNIL, en tant que « chef de file », a adopté sa première décision de sanction en coopération avec d'autres autorités de contrôle européennes, en réponse à plusieurs manquements au RGPD par la société SPARTOO.*

La société SPARTOO est spécialisée dans le secteur de la vente en ligne de chaussures. Pour cette activité, elle dispose d'un site web accessible dans treize pays de l'Union européenne.

La CNIL a contrôlé la société en mai 2018, et a constaté des manquements concernant les données des clients, des prospects et des salariés. La Présidente de la CNIL a donc décidé d'engager une procédure de sanction à l'encontre de la société en 2019.

**Les clients et prospects de la société concernés étant situés dans plusieurs pays européens, la CNIL a coopéré tout au long de la procédure avec les autres autorités européennes concernées en vue de l'adoption de la décision de sanction.**

Sur la base des investigations menées, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – a considéré que la société avait manqué à plusieurs obligations prévues par le RGPD :

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Spartoo SAS

**Когда:** 2020.08

**За что:** нарушение ст. 5(1)(c) и (e), 13, 32 GDPR

**Как:** штраф €250,000 и 3 месяца на устранение нарушений

**Причина:** контролер нарушил принцип минимизации данных, а также хранил данные дольше, чем это было необходимо, а также не выполнил обязательство по информированию субъектов и не принял адекватные меры для обеспечения безопасности данных.

В свете целей обработки данных для обучения работников и предотвращения мошенничества, CNIL считает, что постоянная запись телефонных разговоров с работниками службы поддержки клиентов, запись банковских реквизитов клиентов и сбор медицинских карт клиентов являются чрезмерными и, таким образом, нарушает принцип минимизации данных.

Нарушение затронуло 3 миллиона действующих клиентов и 25 миллионов потенциальных клиентов.

## 779 Штраф за нереализацию права субъекта на отзыв согласия



**Кто:** l’Autorité de protection des données (Бельгия)

**Кого:** Proximus (телеком оператор)

**Когда:** 2020.08

**За что:** нарушение ст. 5, 6, 7, 12, 13, 24, 95 GDPR, ст. 12 e-Privacy Directive

**Как:** штраф €20,000

**Причина:** гражданин Бельгии обратился к компании с запросом на отзыв публикации его персональных данных в публичном справочнике, а также в справочниках других издателей, которым компания передавала персональные данные субъекта. Компания подтвердила исполнение запроса. Однако несколько месяцев спустя субъект обнаружил свои данные в справочниках компании и других издателей.

Таким образом, компания (как контролер) не обеспечила наличие правового основания обработки персональных данных после отзыва согласия субъекта, не предоставила субъекту информацию во время и после получения запроса, а также не исполнила права субъекта должным образом

## 780 Штраф за передачу персональных данных на флешках

**DATATILSYNET**

Du er her: [Forside](#) / [Presse og nyheder](#) / [Nyhedsarkiv](#) / [2020](#) / [aug](#) / [Datatilsynet](#)

### Datatilsynet indstiller PrivatBo til bøde

Publiceret 04-08-2020

Nyhed

PrivatBo er blevet anmeldt til politiet, da Datatilsynet vurderer, at administrationselskabet ikke har levet op til kravene om et passende sikkerhedsniveau i databeskyttelsesforordningen (GDPR).



Datatilsynet har indstillet PrivatBo A.M.B.A. af 1993 til en bøde på 150.000 kr. efter videregivelse af lejeres fortrolige oplysninger.

**Кто:** Datatilsynet (Дания)

**Кого:** PrivatBo (финансовая компания)

**Когда:** 2020.08

**За что:** нарушение ст.32 GDPR

**Как:** штраф €20,150

**Причина:** компания в рамках содействия жилищному фонду в продаже объектов недвижимости предоставила материалы по рассматриваемым объектам недвижимости жильцам на 424 флешках, но вот «и знать не знала», что в материалах содержались персональные данные (в том числе данные об арендной плате, депозитах с указанием адресов) текущих арендаторов. Регулятор посчитал, что компания не реализовала достаточные организационные и технические меры по защите персональных данных (ТОМs).

## Штраф за обработку персональных данных, несовместимую с первоначальной целью



Datatilsynet

### Vedtak om overtredelsesgebyr til Statens vegvesen

Datatilsynet har gitt Statens vegvesen et overtredelsesgebyr på 400 000 kroner for å ha behandlet personopplysninger til formål som er uforenlige med det opprinnelige formålet, og for ikke å ha slettet kameraopptak etter 7 dager.

Bakgrunnen for gebyret er at det i omfattende grad har blitt innhentet og brukt personopplysninger fra fastmonterte veikamera for å overvåke kontraktsparter, ansatte, underleverandører og ansatte hos underleverandørene.

Bruk av slike bilder til dokumentasjon av kontraktsbrudd flere måneder etter at forholdet har skjedd, er ikke forenlig med det sikkerhetsformålet som Veitrakksentralens overvåking er begrunnet med, da den overvåkingen er ment å muliggjøre umiddelbare sikkerhetstiltak. Det er derfor ikke anledning til å benytte opptakene til andre formål slik som kontraktsoppfølging.

I vurderingen av om denne bruken av opptakene er forenlig/uforenlig med det opprinnelige formålet, har Datatilsynet lagt stor vekt på at den nye bruken er til betydelig ulempe for kontraktøren med ansatte, og at det ligger betydelig utenfor hva kontraktøren kan forvente at personopplysningene skal brukes til.

**Кто:** Datatilsynet (Норвегия)

**Кого:** Statens vegvesen (Государственное управление автомобильных дорог Норвегии)

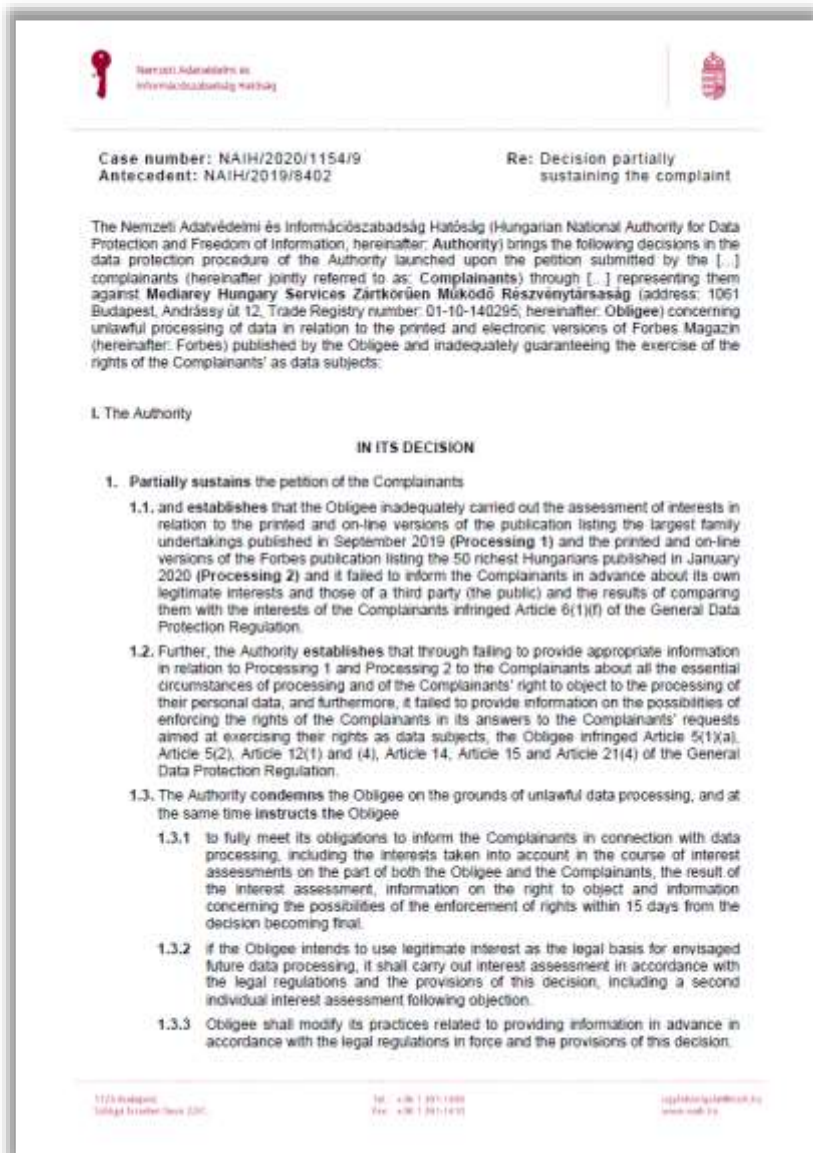
**Когда:** 2020.08

**За что:** нарушение ст. 5(1)(b) GDPR

**Как:** возможный штраф €37,400

**Причина:** Управление использовало систему видеонаблюдения за дорожной сетью (Veitrakksentralen) для контроля действий своих подрядчиков, субподрядчиков и их работников. Использование полученных записей с камер видеонаблюдения для документирования нарушений контрактов между Управлением и его контрагентами через несколько месяцев после возникновения таких нарушений несовместимо с целью обеспечения безопасности, для которой оправдано использование Veitrakksentralen, поскольку эта система предназначена для обеспечения безопасности дорожного движения.

## Штраф СМИ за публикацию персональных данных без проведения LIA



**Кто:** Nemzeti Adatvédelmi és Információszabadság Hatóság (Венгрия)

**Кого:** Mediarey Hungary Services Zrt. (Forbes)

**Когда:** 2020.07

**За что:** нарушение ст. 5(1)(a), 5(2), 6(1)(f), 12(1) и (4), 14, 15, 21(1) и (4) GDPR

**Как:** штраф €12,600

**Причина:** СМИ опубликовало рейтинг 50 богатейших граждан Венгрии, основанием для обработки был законный интерес контролера, но СМИ не провело предварительную оценку законного интереса (Legitimate Interest Assessment).

А ещё компания не проинформировала субъектов обо всех возможных последствиях для субъекта при обработке его данных, а также о возможности исполнения прав субъектов, в том числе о праве возразить против обработки данных.

## Штраф за Welcome Back Talks и чрезмерный контроль персонала



**Кто:** Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Германия)

**Кого:** Hennes & Mauritz Online Shop A.B. & Co. KG

**Когда:** 2020.09

**За что:** нарушение ст. 5 и 6 GDPR

**Как:** штраф €35,258,708

**Причина:** обязательная корпоративная практика Welcome Back Talks, связанная с профилированием, записью и постоянным хранением в электронной системе компании бесед супервайзеров с работниками о деталях их личной жизни, семье, заболеваниях, религиозных убеждениях. Также практиковалось предоставление доступа к этим записям более 50 менеджерам по компании и принятие значимых решений по работникам на основании этих данных.

## Штраф за незаконный утечку медицинских данных из-за «человеческой ошибки»

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** поликлиника «Università Campus Bio-medico di Roma»

**Когда:** 2020.10

**За что:** нарушение ст. 5(2)(a) и (f), 9 GDPR

**Как:** штраф €20,000

**Причина:** поликлиника уведомила надзорный орган в соответствии со статьей 33 GDPR об утечке данных пациентов в отношении системы, через которую можно получить доступ к медицинским онлайн-отчетам. Было обнаружено, что 39 пациентов, получая доступ к своим медицинским онлайн-отчетам через смартфон, также могли получить доступ к данным других 74 пациентов, содержащим медицинские отчеты и результаты медицинских осмотров. Поликлиника указала, что причиной утечки стала человеческая ошибка при интеграции двух ИТ-систем.





## Штраф за отсутствие контроля доступа к медицинской информации



SYKEHUSET ØSTFOLD HF  
Postboks 300  
1714 GRÅLUM

Deres referanse  
19/00251

Vår referanse  
20/02291-4

Dato  
22.10.2020

### Vedtak om overtredelsesgebyr og pålegg

Datatilsynet viser til tidligere korrespondanse i forbindelse med melding om brudd på personopplysningsikkerheten (avviksmelding) med referanse AR300186895, som dere sendte 14.01.2019.

I brev datert 16.07.2019 ba vi om en redegjørelse for flere forhold knyttet til avviket. Sykehuset Østfold HF redegjorde for saken i brev av 13.08.2019.

Den 22.06.2020 varslert vi Sykehuset Østfold HF om at vi ville vurdere å fatte vedtak om overtredelsesgebyr og pålegg. Sykehuset har kommentert varselet i brev datert 29.06.2020.

Vi beklager den lange saksbehandlingstiden.

### 1. Vedtak om overtredelsesgebyr og pålegg

Datatilsynet har i dag fattet følgende vedtak:

- 1. I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 andre ledd og pasientjournalloven § 29, jf. personvernforordningen artikkel 83, pålegges Sykehuset Østfold HF å betale et overtredelsesgebyr på 750 000 NOK – syv hundre og femti tusen norske kroner – til statskassen, for overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32, jf. personopplysningsloven § 26 første ledd, jf. personvernforordningen artikkel 24, og pasientjournalloven §§ 22 og 23.*
- 2. I medhold av personvernforordningen artikkel 58 nr. 2 bokstav d, pålegges Sykehuset Østfold HF å tilse at styringssystemet for behandling av personopplysninger er egnet til å ivareta kravene i personvernregelverket og pasientjournalloven. Vi viser særlig til rutinene for tilgangskontroll og lagring av personopplysninger. Styringssystemet må innebære oppfølging av at rutinene følges, herunder oppfølging av at kun sikre systemer brukes ved*

Postadresse: Postboks 458 Sentrum 0105 OSLO  
Kontordresse: Tollbugt 3  
Telefon: 22 39 69 00  
Telefaks: 22 42 23 50  
Org.nr: 974 761 467  
Hjemmeside: www.datatilsynet.no

**Кто:** Datatilsynet (Норвегия)

**Кого:** больница «Østfold HF»

**Когда:** 2020.10

**За что:** нарушение ст. 5, 6 и 32 GDPR

**Как:** штраф €69,150

**Причина:** в ходе расследования выяснилось, что определенные журналы пациентов не хранятся и не контролируются больницей должным образом, а данные хранятся намного дольше, чем это было необходимо. В частности, было выявлено отсутствие контроля доступа к медицинской информации и не осуществления журналирования доступа к ней. Доступ к медицинским данным был предоставлен 118 работникам больницы, хотя большинство из них формально не нуждались в таком доступе. Надзорный орган пришел к выводу, что по итогам расследования больница «создала систему контроля доступа, достаточную для предотвращения подобных нарушений в будущем».

## 786 Штраф за незаконную обработку данных в МВД

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Министерство внутренних дел Италии

**Когда:** 2020.10

**За что:** нарушение ст. 5 и 16 GDPR

**Как:** штраф €50,000

**Причина:** полицейское управление МВД Италии своевременно не отреагировало на запрос субъекта об уточнении его персональных данных, обрабатываемых в базах данных МВД, и продолжило обрабатывать неточные данные.





**RECHTSINFORMATIONSSYSTEM DES BUNDES** RIS

### Datenschutzbehörde

Hinweis: Es wurden keine Rechtssätze für das Dokument 'DSBT\_20201019\_2020\_0\_550\_322\_00' im RIS-Datenbestand gefunden.

<b>Entscheidende Behörde</b> <a href="#">Datenschutzbehörde</a>	<b>Dokumenttyp</b> Entscheidungstext
<b>Entscheidungsart</b> Verwaltungsstraferkennnis/Verwarnung /Ermahnung	<b>Geschäftszahl</b> 2020-0.550.322
<b>Entscheidungsdatum</b> 19.10.2020	

**Anfechtung beim BVwG/VwGH/VfGH**  
Dieses Straferkennnis ist rechtskräftig.

**Norm**  
DSGVO Art4 Z2  
DSGVO Art5 Abs1 lita  
DSGVO Art6 Abs1  
DSGVO Art83 Abs5 lita  
DSGVO ErwGr47  
DSGVO ErwGr148  
VStG §19 Abs1

**Text**  
GZ: 2020-0.550.322 vom 19. Oktober 2020 (Verfahrenszahl: DSB-D550.249)  
[Anmerkung Bearbeiter: Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), etc., sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

**Straferkennnis**  
**Beschuldigter: A\*\*\* F\*\*\* (geb. TT.MM.JJJJ), [PLZ] [Ort], [Straße] [HNr.]**

**Tatzeit:** TT.MM.2019, 19:35 Uhr  
**Tatort:** [PLZ] [Ort], [Straße, ONr.] (WC-Anlagen im Obergeschoß nächst der Polizeiinspektion \*\*\*)

Sie haben als Verantwortlicher im Sinne von Art 4 Z 7 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, im Folgenden: DSGVO), ABl. Nr. L 119 vom 4.5.2016 S 1, zur oben angegebenen Tatzeit am oben bezeichneten Tatort folgende Verwaltungsübertretung(en) verwirklicht:

Sie haben eine weibliche Person, während diese eine der WC-Kabinen benutzte, im Rahmen einer Bilddatenverarbeitung erfasst, indem Sie unter einer WC-Kabinentrennwand ein Mobiltelefon (Smartphone mit Kamerafunktion) hindurchgeschoben haben, wobei der Bildschirm des Mobiltelefons dabei nach oben zeigte und die Frontkamera des Mobiltelefons während des gesamten Vorganges aktiv war und somit Bilddaten von der betroffenen Person verarbeitet wurden.

Durch diese rechtsgrundlose Vornahme einer Bilddatenverarbeitung haben Sie gegen die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 lit. a DSGVO,

**Кто:** Österreichische Datenschutzbehörde (Австрия)

**Кого:** частное лицо

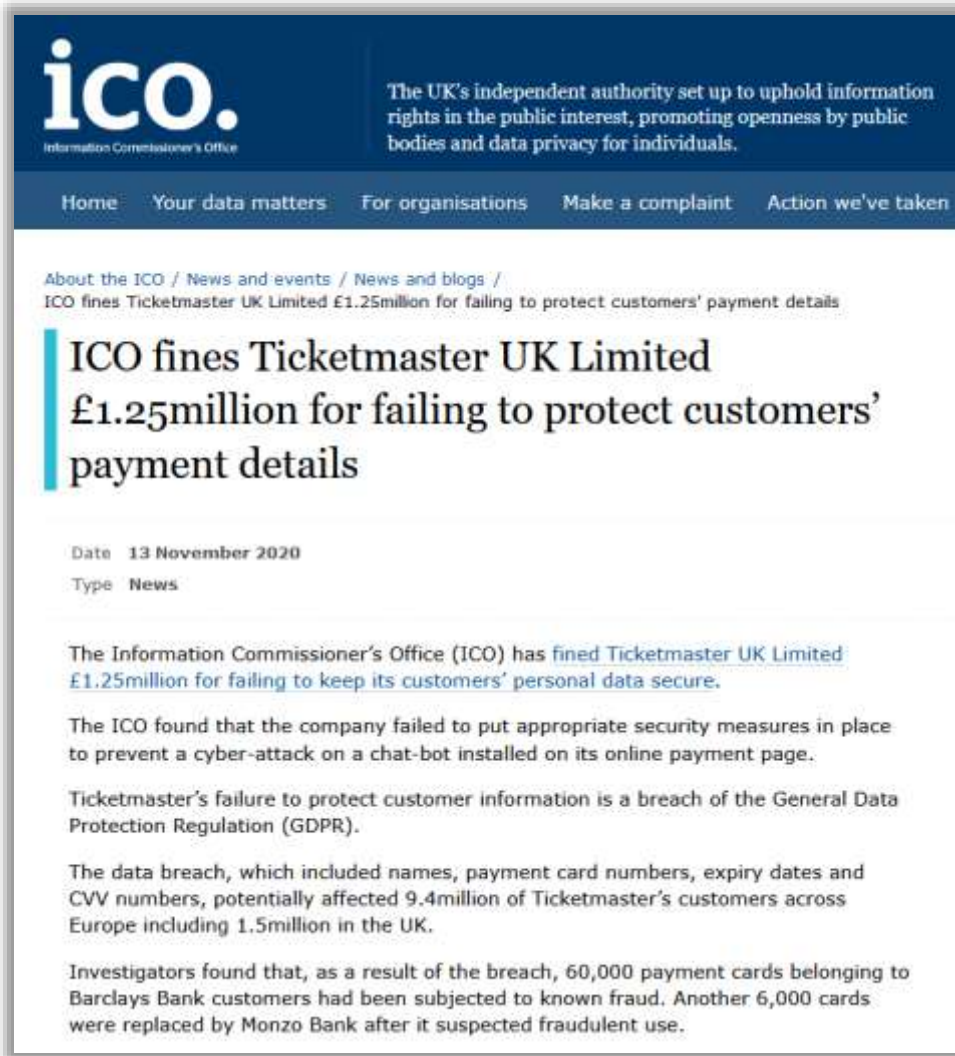
**Когда:** 2020.10

**За что:** нарушение ст. 5(1) а) и 6 GDPR

**Как:** штраф €150 или тюремное заключение на 9 часов (при невыплате штрафа)

**Причина:** частное лицо осуществило видеосъемку женщины, когда она пользовалась одной из кабин туалета, поместив сотовый телефон (смартфон с функцией камеры) под перегородку кабины туалета, при этом экран был направлен вверх, а передняя камера мобильного телефона была активна во время весь процесс.

## Штраф за недостаточные меры защиты чат-бота, используемого на странице оплаты



The screenshot shows the homepage of the Information Commissioner's Office (ICO). The header includes the ICO logo and the tagline: "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." Below the header is a navigation menu with links: Home, Your data matters, For organisations, Make a complaint, and Action we've taken. The main content area features a news article titled "ICO fines Ticketmaster UK Limited £1.25million for failing to protect customers' payment details". The article is dated 13 November 2020 and is categorized as News. The text of the article states that the ICO has fined Ticketmaster UK Limited £1.25million for failing to keep its customers' personal data secure. It details that the ICO found the company failed to put appropriate security measures in place to prevent a cyber-attack on a chat-bot installed on its online payment page. Ticketmaster's failure to protect customer information is a breach of the General Data Protection Regulation (GDPR). The data breach, which included names, payment card numbers, expiry dates and CVV numbers, potentially affected 9.4million of Ticketmaster's customers across Europe including 1.5million in the UK. Investigators found that, as a result of the breach, 60,000 payment cards belonging to Barclays Bank customers had been subjected to known fraud. Another 6,000 cards were replaced by Monzo Bank after it suspected fraudulent use.

**Кто:** Information Commissioner's Office (Великобритания)

**Кого:** Ticketmaster

**Когда:** 2020.11

**За что:** нарушение ст. 5, 25 GDPR

**Как:** штраф €1,400,000

**Причина:** в результате действий злоумышленников, которые стали возможными благодаря взлому чат-бота компании Ticketmaster на странице оплаты билетов, были скомпрометированы платежные данные (имена, номера платёжных карт, срок действия карт, CVV) 9,4 млн субъектов со всей Европы (1,5 млн из UK, поэтому ICO был ведущим регулятором по этому вопросу). Хотя контролёр еще в 2018 году получал сообщения от своих партнеров о подозрительной активности, но её источник не был современно выявлен и нейтрализован компанией.

## Штраф за незаконный прямой маркетинг и отсутствие контроля над законностью получения контактных данных

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Vodafone

**Когда:** 2020.11

**За что:** нарушение ст. 5, 6 и 25 GDPR

**Как:** штраф €12,251,601 и запрет на обработку данных в маркетинговых или коммерческих целях, если такие данные получены от третьих лиц, не получивших свободного, конкретного и осознанного согласия пользователей на раскрытие данных

**Причина:** компания не получила согласие субъектов на маркетинговые активности (звонки с целью продвижения услуг Vodafone). Причём сами рекламные звонки выполнялись с фейковых номеров, не зарегистрированных в национальной базе сотовых операторов Италии. А базу потенциальных клиентов компания приобрела у сторонних организаций. Также компания не имплементировала необходимые меры по защите данных (субъекты получали от компаний, действующих от имени Vodafone, запросы по WhatsApp), не придерживалась принципов подотчетности и Privacy by Design.

**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

### Telemarketing aggressivo. Dal Garante privacy sanzione a Vodafone per 12 milioni 250 mila euro

Telemarketing aggressivo. Dal Garante privacy sanzione a Vodafone per 12 milioni 250 mila euro.

Il Garante per la protezione dei dati personali - composto da Pasquale Stanzone, Geneva Corina Ferroni, Agostino Ghiglia e Guido Scorza - [ha ordinato a Vodafone il pagamento di una sanzione di oltre 12 milioni e 250 mila euro](#) per aver trattato in modo illecito i dati personali di milioni di utenti a fini di telemarketing. Oltre al pagamento della multa, la società dovrà adottare una serie di misure dettate dall'Autorità per conformarsi alla normativa nazionale ed europea sulla tutela dei dati.

Il provvedimento conclude una complessa istruttoria avviata dal Garante a seguito di centinaia di segnalazioni e reclami di utenti che lamentavano continui contatti telefonici indesiderati, effettuati da Vodafone e dalla sua rete di vendita, per promuovere i servizi di telefonia e internet offerti dall'azienda.

Gli accertamenti svolti dall'Autorità hanno evidenziato importanti criticità "di sistema" - che riguardano la violazione non solo dell'obbligo del consenso, ma anche dei fondamentali principi di responsabilizzazione e di implementazione delle tutele privacy fin dalla fase di progettazione dei trattamenti, stabiliti dal Regolamento Ue. Criticità riconducibili al complesso delle operazioni svolte dalla società nei confronti sia dell'intera base clienti di Vodafone, sia del più ampio ambito dei potenziali utenti del settore delle comunicazioni elettroniche.

Nel corso dell'istruttoria è emerso, in particolare, un allarmante fenomeno di utilizzo di numerazioni fittizie o comunque non censite nel Registro degli Operatori di Comunicazione (Roc) per realizzare i contatti promozionali. Un fenomeno, avvertito dalla stessa Vodafone, che sembra ricondursi in massima parte ad un "sottobosco" di call center abusivi, che effettuano attività di telemarketing in totale spregio delle disposizioni in materia di protezione dei dati personali.

Ulteriori profili di violazione sono stati rilevati nella gestione delle liste dei nominativi da contattare acquisite da fornitori esterni. Liste che i partners commerciali di Vodafone avevano ricevuto da altre aziende e trasferito all'operazione telefonica senza il necessario consenso libero, informato e specifico degli utenti.

Sono risultate inadeguate anche le misure di sicurezza dei sistemi di gestione della clientela, profilo sul quale l'Autorità aveva già ricevuto numerosi reclami e segnalazioni da parte di clienti che erano stati contattati da sediioni operatori Vodafone, i quali chiedevano l'invio di documenti di identità mediante Whatsapp, probabilmente con finalità di spamming, phishing o per la realizzazione di altre attività fraudolente.

Alla luce delle violazioni riscontrate, il Garante Privacy ha applicato una sanzione di 12.251.601,00 euro.

L'Autorità ha quindi ordinato a Vodafone di introdurre dei sistemi che consentano di comprovare che i trattamenti a fini di telemarketing si svolgono nel rispetto delle disposizioni in materia di consenso. La società dovrà inoltre dimostrare che i contatti siano attivati solo a seguito di chiamate promozionali effettuate dalla sua rete di vendita, attraverso numerazioni censite e iscritte al Roc. Vodafone dovrà anche introdurre le misure di sicurezza al fine di impedire accessi abusivi al database dei clienti e fornire pieno riscontro alle richieste di esercizio dei diritti formulate da alcuni utenti.

Il Garante, infine, ha vietato a Vodafone ogni ulteriore trattamento di dati con finalità promozionali o commerciali svolto mediante l'acquisizione di liste anagrafiche da soggetti terzi, senza che questi ultimi abbiano acquisito un consenso specifico, libero e

## Штраф за незаконное использование видеонаблюдения без проведения DPIA



The screenshot shows the homepage of the Swedish Datainspektionen (Data Protection Authority). The header includes the logo, navigation links (OM OSS, KONTAKTA OSS, PRESS, A-Ö, IN ENGLISH), and a search bar. A red navigation bar contains the categories: AKTUELLT, FRÅGOR OCH SVAR, VÄGLEDNINGAR, and LAGAR OCH REGLER. The main content area features a breadcrumb trail: Start → Nyheter → Sanktionsavgift för olaglig kamerabevakning på LSS-boende. Below this is the publication date: Publicerad 2020-11-25. The article title is "Sanktionsavgift för olaglig kamerabevakning på LSS-boende". The sub-headline reads: "Datainspektionen utfärdar en sanktionsavgift på 200 000 kronor mot Gnosjö kommun med anledning av olaglig kamerabevakning på ett LSS-boende." The main text states: "Datainspektionen har tagit emot ett klagomål från en anhörig till en boende på ett LSS-boende i Gnosjö kommun som gör gällande att den boende kameraövervakas olagligt. Myndigheten har inlett en granskning av LSS-boendet och kan konstatera att den boende kamerabevakats i sitt sovrum i strid med dataskyddsförordningen, GDPR, och kamerabevakningslagen." A quote from Jeanette Bladh Gustafson, a jurist at the authority, follows: "– Den boende har kamerabevakats i hemmets mest privata sfär, vilket gör att vi bedömer att kamerabevakningen har inneburit ett alltför stort intrång i den boendes personliga integritet, säger Jeanette Bladh Gustafson som är jurist på Datainspektionens kameragrupp." The final paragraph mentions: "Socialutskottet i Gnosjö, som ansvarar för LSS-boendet, har uppgett att den boendes sjukdomsbild har skapat stora svårigheter såväl för den boende själv som för personalen och att det har uppkommit situationer där det varit fråga om risk för den boendes liv och hälsa. Det har även förekommit att personal kommit till skada."

**Кто:** Datainspektionen (Швеция)

**Кого:** муниципалитет Гносе

**Когда:** 2020.11

**За что:** нарушение ст. 5, 6 и 12 GDPR

**Как:** штраф €19,500


**Причина:** штраф был наложен по жалобе родственника жильца одного из муниципальных домов, в спальне которого была установлена камера видеонаблюдения. Комитет по социальным вопросам муниципалитета заявил, что болезнь жильца создала большие трудности как для него самого, так и для окружающих людей. Надзорный орган решил, что нет никаких юридических оснований для использования видеонаблюдения в данной ситуации с учетом того, что DPIA не было проведено и что субъект не был проинформирован о видеонаблюдении.

## Штрафы за нарушения GDPR, включая непредставление информации и использование cookies без согласия

**CNIL.**

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

MES DÉMARCHES | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL |   

 > Sanctions de 2 250 000 euros et de 800 000 euros pour les sociétés CARREFOUR FRANCE et CARREFOUR BANQUE

### Sanctions de 2 250 000 euros et de 800 000 euros pour les sociétés CARREFOUR FRANCE et CARREFOUR BANQUE

26 novembre 2020

*Saisie de plusieurs plaintes, la CNIL a sanctionné deux sociétés du groupe CARREFOUR pour des manquements au RGPD concernant notamment l'information délivrée aux personnes et le respect de leurs droits.*

Saisie de plusieurs plaintes à l'encontre du groupe CARREFOUR, la CNIL a effectué des contrôles entre mai et juillet 2019 auprès des sociétés CARREFOUR FRANCE (secteur de la grande distribution) et CARREFOUR BANQUE (secteur bancaire). À cette occasion, la CNIL a constaté des manquements concernant le traitement des données des clients et des utilisateurs potentiels. La Présidente de la CNIL a donc décidé d'engager une procédure de sanction à l'encontre de ces sociétés.

À l'issue de cette procédure, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – a effectivement considéré que les sociétés avaient manqué à plusieurs obligations prévues par le RGPD.

Elle a ainsi sanctionné la société CARREFOUR FRANCE d'une amende de 2 250 000 euros et la société CARREFOUR BANQUE d'une amende de 800 000 euros. En revanche, elle n'a pas prononcé d'injonction dès lors qu'elle a constaté que des efforts importants avaient permis la mise en conformité sur tous les manquements relevés.

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Carrefour France и Carrefour Banque

**Когда:** 2020.11

**За что:** нарушение ст. 5, 12, 13, 15, 17, 21, 32, 33 GDPR

**Как:** штрафы €2,250,000 и €800,000

**Причина:** сведи прочих нарушений, особо можно отметить следующие:

- информация об обработке данных, предоставленная пользователям сайтов [carrefour.fr](https://www.carrefour.fr) и [carrefour-banque.fr](https://www.carrefour-banque.fr), а также людям, желающим присоединиться к программе лояльности или карте Pass, была труднодоступной, непонятной (информация написана в общих и неточных терминах, иногда с использованием излишне сложных формулировок) и неполной (в отношении продолжительности хранения данных);
- при переходе пользователей на сайты [carrefour.fr](https://www.carrefour.fr) и [carrefour-banque.fr](https://www.carrefour-banque.fr) несколько файлов cookie, связанных с рекламными активностями, автоматически загружались на пользовательские устройства без получения предварительного согласия пользователей.

## Штрафы за нарушение принципа проектируемой защиты данных (Data Protection by Design)

### The Estonian Data Protection Inspectorate obliged e-pharmacies to immediately terminate access to another person's prescription information



🕒 Tuesday, 8 December, 2020 EE

On 30 November, the Estonian Data Protection Inspectorate issued a precept, granted in a warning, with a one-day compliance deadline and a penalty of 100,000 euros to three pharmacy chains that allowed viewing in the e-pharmacy environment the current prescriptions of another person without their consent on the basis of access to their personal identification code.

'We considered it necessary to urgently suspend the display of valid prescriptions to third persons in e-pharmacy environments on the basis of personal identification codes, as there is no legal basis for such display,' said Maris Juha, Supervisory Director.

It must be possible to buy prescription medicine for other people, but the solution must ensure that the pharmacist is sure that the prescription information is accessed with the consent of the prescription holder. The Estonian Data Protection Inspectorate cannot approve the violation of data protection requirements in the e-pharmacy environments of the three pharmacy chains.

When the lawyer of the Data Protection Inspectorate checked the e-pharmacy environments, they were able to gain quick access to the prescription information of other persons, using the chat window. First, they had to choose in the chat window whether they requested their own prescription information or the prescription information of someone else, and if they entered the personal identification code of another person, the corresponding information became available. Only one of the three pharmacy chains had a solution which required prior confirmation of whether the person has the right to view the above information. However, another person's justification is not equivalent to the voluntary consent of the prescription holder, because the e-pharmacy cannot check whether and for what purpose consent has been given and whether it has been given voluntarily.

**Кто:** Andmekaitse Inspektsioon (Эстония)

**Кого:** электронные аптеки Apotheka, Südameapteek и Azeta.ee

**Когда:** 2020.11

**За что:** нарушение ст. 5, 6 и 25 GDPR

**Как:** штраф €100,000 и предписание о приостановке противоправной обработки данных

**Причина:** третьи лица с помощью идентификационных кодов клиентов электронных аптек могли получить доступ к данным о выданных клиентам рецептах без согласия клиентов. Так, работник Инспекции по защите данных посетил вебсайт электронной аптеки, где он смог получить быстрый доступ к информации о рецептах других лиц с помощью онлайн чата.



## Штраф за утечку персональных данных 3,2 млн. норвежцев



### Varsel om overtredelsesgebyr til Norges idrettsforbund

Datatilsynet har sendt Norges idrettsforbund (NIF) et varsel om overtredelsesgebyr på 2,5 millioner kroner. Bakgrunnen for saken er at personopplysninger om 3,2 millioner nordmenn ble liggende tilgjengelig på nett i 87 dager etter en feil i forbindelse med test av en skyløsning.

Datatilsynet vurderer at Norges idrettsforbund ikke hadde iverksatt gode nok sikkerhetsrutiner for testingen, og at det ikke var nødvendig å teste med et slikt omfang av personopplysninger.

– NIF har ikke satt inn de tekniske og organisatoriske tiltakene som skulle til. Omtrent halvparten av Norges befolkning er berørt av avviket, mange av dem er barn. Barn er en spesielt sårbar gruppe, noe vi har vektlagt spesielt i vår vurdering, uttaler direktør i Datatilsynet, Bjørn Erik Thon.

#### Bakgrunn for saken

Saken startet med en avviksmelding til Datatilsynet fra forbundet 20. desember 2019, etter at Nasjonalt Cybersikkerhetssenter hadde varslet dem at personopplysningene lå tilgjengelig på en offentlig *IP-adresse*. Avviket oppsto da det skulle testes løsninger i forbindelse med flytting av database fra et fysisk servermiljø og opp i skyen.

Personopplysningene som var eksponert var navn, kjønn, fødselsdato, adresse, telefonnummer, e-post og klubbtilhørighet. Av de 3,2 millioner personene som var berørt av avviket, var 486 447 barn i alderen 3-17 år. Datatilsynet har ikke opplysninger om at uvedkommende faktisk har utnyttet avviket.



Publisert: 07.12.2020

**Кто:** Datatilsynet (Норвегия)

**Кого:** Norges idrettsforbund (Норвежская спортивная конфедерация)

**Когда:** 2020.12

**За что:** нарушение ст. 5 и 32 GDPR

**Как:** штраф €236,500

**Причина:** персональные данные 3,2 млн. норвежцев оказались в открытом доступе в сети «Интернет» на протяжении 87 дней после технической ошибки в связи с тестированием облачной платформы спортивной конфедерации Норвегии. Причиной утечки было то, что конфедерация не внедрила достаточно хороших процедур безопасности для тестирования и что тестирование проводилось с полным объемом данных, хотя в этом не было необходимости. Интересно, что утечку обнаружил Национальный центр кибербезопасности Норвегии.

## Штраф в €100,000,000 за неправомерное размещение рекламных файлов cookie



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Google LLC и Google Ireland Limited

**Когда:** 2020.12

**За что:** нарушение ст. 5, 6 и 13 GDPR

**Как:** штрафы €60,000,000 на Google LLC и €40,000,000 Google Ireland Limited, 3 месяца на устранение, €100,000 за каждый день просрочки в устранении нарушения

**Причина:** размещение рекламных файлов cookie на компьютерах пользователей при использовании поисковой системы google.fr без предварительного согласия или надлежащего информирования пользователей (50 млн. субъектов).

## Штраф в €35,000,000 за неправомерное размещение рекламных файлов cookie

**CNIL.**

*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL |   

### Cookies : sanction de 35 millions d'euros à l'encontre d'AMAZON EUROPE CORE

10 décembre 2020

*Le 7 décembre 2020, la formation restreinte de la CNIL a sanctionné la société AMAZON EUROPE CORE d'une amende de 35 millions d'euros pour avoir déposé des cookies publicitaires sur les ordinateurs d'utilisateurs à partir du site amazon.fr sans consentement préalable et sans information satisfaisante.*



Entre le 12 décembre 2019 et le 19 mai 2020, la CNIL a effectué plusieurs contrôles, notamment en ligne, concernant le site web amazon.fr. Ces vérifications ont permis de constater que lorsqu'un utilisateur se rendait sur ce site, des cookies étaient automatiquement déposés sur son ordinateur, sans action de sa part. Plusieurs de ces cookies poursuivaient un objectif publicitaire.

#### Les manquements à la loi Informatique et Libertés

La formation restreinte, organe de la CNIL chargé de prononcer les sanctions, a relevé deux violations à l'article 82 de la loi Informatique et Libertés :

##### Un dépôt de cookies sans recueillir le consentement de l'utilisateur

La formation restreinte a relevé que lorsqu'un internaute se rendait sur l'une des pages du site amazon.fr, un grand nombre de cookies à vocation publicitaire était instantanément déposé sur son ordinateur, c'est-à-dire avant que celui-ci n'exécute la moindre action. Or, la formation restreinte a rappelé que ce type de cookies, non essentiels au service, ne pouvait être déposé qu'après que l'internaute a exprimé son consentement. Elle a considéré que le fait de déposer des cookies concomitamment à l'arrivée sur le site était une pratique qui, par nature, était incompatible avec un consentement préalable.

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Amazon Europe Core

**Когда:** 2020.12

**За что:** нарушение ст. 5, 6 и 13 GDPR

**Как:** штраф €35,000,000, 3 месяца на устранение, €100,000 за каждый день просрочки в устранении нарушения

**Причина:** размещение рекламных файлов cookie на компьютерах пользователей при использовании поисковой системы amazon.fr без предварительного согласия или надлежащего информирования пользователя.



**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** Virgin Mobile Polska


**Когда:** 2020.12

**За что:** нарушение ст. 5(1)(f), 5(2), 25(1), 32(1)(b), 32(1)(d), 32(2) GDPR


**Как:** штраф €444,000

**Причина:** контролёр не предпринял соответствующие технические и организационные меры безопасности, соответствующие риску обработки данных с использованием ИТ-систем. Ранее контролёр уведомил надзорный орган об имевшем место в декабре 2019 года неправомерном доступе злоумышленников к персональным данным абонентов компании (было скомпрометировано 142,222 записей в отношении 114,963 абонентов, включая имя и фамилию, регистрационный номер PESEL, серию и номер удостоверения личности, номер телефона, идентификационный номер налогоплательщика и название юридического лица).

## Штраф за ненадлежащее получение согласий пользователей мобильного приложения



agencia  
española  
protección  
datos



1/124

- Procedimiento N°: PS/00070/2019

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

**PRIMERO:** Con fecha 16/10/2018, tuvo entrada en esta Agencia una reclamación presentada por D. A.A.A. (en lo sucesivo el reclamante 1), contra la entidad BANCO BILBAO VIZCAYA ARGENTARIA, S.A. (en lo sucesivo BBVA), por el envío a su línea de telefonía móvil, en fecha 11/10/2018, de un SMS promocional. Añade que no ha autorizado el envío de tales mensajes y que figura inscrito en Lista Robinson desde hace tiempo.

Con su reclamación, aporta únicamente copia del SMS objeto de la misma, cuyo texto es el siguiente:

*"Publi BBVA: Tu prestamos HASTA 9.000 EUROS para poner en marcha ya tus proyectos. Info 912975969. https://bbva.info/2xLgPps. No+publi envia BAJA al 217582"*

Esta reclamación fue trasladada a la entidad BBVA. En respuesta a lo manifestado por el reclamante 1, BBVA informa a esta Agencia que el mismo prestó su conformidad al contenido del documento *"Identificación del cliente, tratamiento de datos personales y firma digitalizada"*, suscrito por el reclamante en fecha 07/06/2016, en virtud del cual el cliente consintió el envío de publicidad por parte de BBVA "a través de cualquier medio".

Añade BBVA que, no obstante, vista la reclamación formulada, ha procedido a inhabilitar la opción relativa al envío de comunicaciones comerciales al reclamante 1.

BBVA aporta el documento *"Identificación del cliente, tratamiento de datos personales y firma digitalizada"* suscrito por el denunciante en fecha 07/06/2016.

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Banco Bilbao Vizcaya Argentaria, S.A.

**Когда:** 2020.12

**За что:** нарушение ст. 6, 13 GDPR

**Как:** штраф €5,000,000

**Причина:** мобильное приложение контролера для систем Android предлагало своим пользователям предоставить согласие в целях аналитики, персонализации сервисов, маркетинга и на передачу данных третьим лицам, при этом согласие фактически не являясь добровольным и осознанным, так как «чек-бокс» в форме согласия был активирован по умолчанию. Любопытным является факт того, что ранее DPO контролера получал обращения от пользователей с указанием на эту недобросовестную практику, но банк решил не вносить изменения в процесс получения согласий пользователей.

## Штраф Booking.com за слишком позднее уведомление о нарушении безопасности данных



**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** Booking.com

**Когда:** 2020.12

**За что:** нарушение ст. 33 GDPR

**Как:** штраф €475,000

**Причина:** уведомление о нарушении безопасности данных, имевшее место в 2018 году, было направлено надзорному органу только через 22 дня после того, как оно произошло, хотя установленный законом срок составляет 72 часа.

Утечка данных произошла из-за действий хакеров, которые ранее получили доступ к служебным учетным записям Booking.com работников 40 отелей в ОАЭ. Это привело к компрометации данных о 4,109 клиентах Booking.com, которые бронировали номера в отелях в ОАЭ.

## 799 Штраф за незаконное видеонаблюдение в отношении работников



**Кто:** LfD Niedersachsen (Германия)

**Кого:** notebooksbilliger.de AG

**Когда:** 2021.01

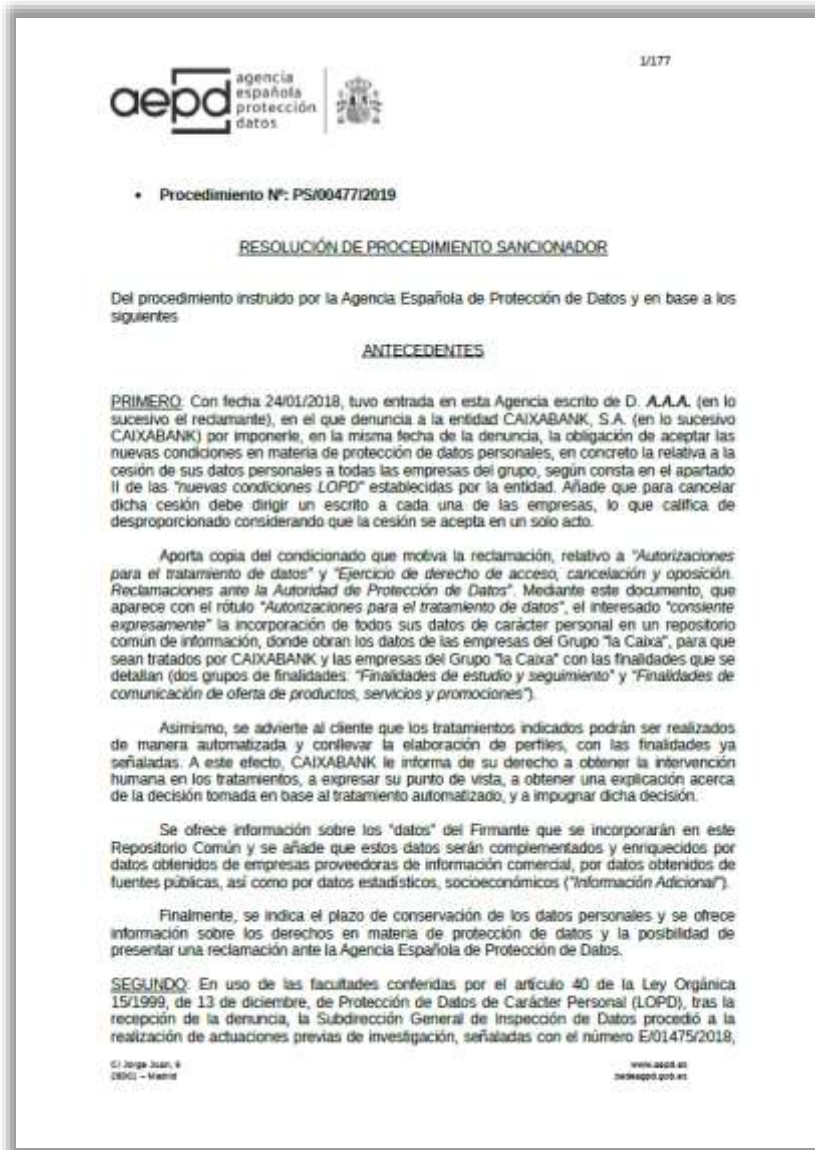
**За что:** нарушение ст. 5, 6 GDPR

**Как:** штраф €10,400,000

**Причина:** контролер осуществлял видеонаблюдение за своими работниками в течение более двух лет без каких-либо юридических оснований. Видеокамеры фиксировали рабочие места, торговые помещения, склады и места общего пользования. Целью CCTV было заявлено предотвращение и расследование уголовных преступлений и отслеживание перемещения товаров на складах.

DPA постановил, что для предотвращения краж компания должна была сначала изучить более иные способы контроля, например, выборочная проверка сумок при покидании работниками помещений предприятия. Кроме того, видеонаблюдение для раскрытия уголовных преступлений также является законным только при наличии обоснованных подозрений в отношении конкретных лиц, и что в этом случае можно их отслеживать с помощью CCTV в течение ограниченного периода времени.

## Штраф за недостаточное информирование субъектов и нарушения в правовых основаниях обработки данных



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** CaixaBank S.A.

**Когда:** 2021.01

**За что:** нарушение ст. 6, 13 и 14 GDPR

**Как:** штрафы €4,000,000 и €2,000,000

**Причина:** распространяемая CaixaBank в различных документах и каналах информация об обработке данных не была единообразной, в политике конфиденциальности использовалась неточная терминология, а информация о категориях обрабатываемых персональных данных, профилях пользователей, использовании данных, сроках хранения данных и способах реализации прав субъектов была неполной.


Банк не предоставил достаточного обоснования для обработки данных на основании законного интереса, а также не выполнял требованиям в отношении получения конкретных, недвусмысленных и информированных согласий. В постановлении AEPD также указывается, что банк осуществлял незаконную передачу клиентских данных аффилированным компаниям.

<https://www.aepd.es/es/documento/ps-00477-2019.pdf>

[https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank-sa\\_fr](https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank-sa_fr)



## Штраф за незаконную автоматическую пересылку электронной корреспонденции работника



[Lover og regler](#) / [Sentrale avgjørelser](#) / 2021

### Får gebyr for videresending av e-post

Datatilsynet har ilagt en virksomhet et overtredelsesgebyr på 400 000 kroner for ulovlig automatisk videresending av en ansatts e-postkasse.


Bakgrunn for saken er en klage fra en arbeidstaker som opplevde at arbeidsgiveren hadde aktivert automatisk videresending av vedkommende sin e-postkasse i virksomheten.

#### Mangler rettslig grunnlag

Den automatiske videresendingen ble aktivert i forbindelse med arbeidstakerens sykefravær, og varte i over en måned. Etter å ha undersøkt saken nærmere har Datatilsynet konkludert med at videresendingen har skjedd i strid med reglene i forskriften om arbeidsgivers innsyn i e-postkasse og annet elektronisk materiale, samt personvernforordningens krav til rettslig grunnlag, informasjon til [den registrerte](#) og plikten til å vurdere arbeidstakerens protest.


På bakgrunn av dette har Datatilsynet fattet vedtak om at virksomheten må utbedre de skriftlige rutinene for innsyn i e-postkasse, samt et pålegg om å betale et overtredelsesgebyr på 400 000 kroner for den ulovlige videresendingen.

Virksomhetens navn er unntatt offentlighet for å skjerme klagers identitet. Virksomheten har påklaget vedtaket.



#### Kontaktperson

Ole Martin Moe  
juridisk rådgiver



Kontor: [\(+47\) 22 39 89 59](tel:+4722398959)  
E-post: [omm@datatilsynet.no](mailto:omm@datatilsynet.no)

Publisert: 12.01.2021

**Кто:** Datatilsynet (Норвегия)

**Кого:** неназванная компания

**Когда:** 2021.01

**За что:** нарушение ст. 5, 6 GDPR

**Как:** возможный штраф €38,600

**Причина:** расследование было инициировано по жалобе работника, который узнал, что работодатель активировал автоматическую пересылку сообщений из служебной электронной почты этого работника. Пересылка проводилась в связи с подозрениями в отношении обоснованности ухода работника на больничный и длилась более месяца. По мнению надзорного органа, это ущемило права работника на защиту приватности. Компания обжаловала вынесенное решение в суде.



**Datatilsynet**

Aktuelle nyheter 2021

## Vedtak om overtredelsesgebyr til Coop Finnmark

Datatilsynet har fattet vedtak om overtredelsesgebyr på 400 000 kroner til Coop Finnmark SA. Saken gjelder ulovlig deling av et kameraopptak fra en butikk.

Butikksjefen i den aktuelle butikken filmet av overvåkingsopptak med en mobiltelefon, og delte filmen videre. Filmen ble raskt spredd.

Beløpet er uendret etter at vi først sendte varsel i saken.

### Manglet rettslig grunnlag

Enhver behandling av personopplysninger krever et rettslig grunnlag for å være lovlig. Etter å ha undersøkt saken nærmere er Datatilsynets vurdering at Coop Finnmark ikke hadde rettslig grunnlag for butikksjefens deling av opptakene fra overvåkingen.

- Kravet om lovlighet er et grunnleggende prinsipp i *personvernforordningen*, og et brudd på dette prinsippet er alvorlig, forklarer juridisk rådgiver Embla Helle Nerland i Datatilsynet.

Saken ble meldt inn som et brudd på personopplysningssikkerheten (avviksmelding) fra Coop Finnmark SA 10. april 2019, og Datatilsynet varslet overtredelsesgebyret i mars 2020. Coop Finnmark har levert merknader til varselet som nå er ferdigbehandlet hos Datatilsynet.



#### Kontaktperson

Embla Helle Nerland  
juridisk rådgiver

Kontor: + 47 22 39 69 64  
E-post: [ehn@datatilsynet.no](mailto:ehn@datatilsynet.no)



Publisert: 14.01.2021

**Кто:** Datatilsynet (Норвегия)

**Кого:** Coop Finnmark SA

**Когда:** 2021.01

**За что:** нарушение ст. 5, 6 GDPR

**Как:** возможный штраф €38,600

**Причина:** менеджер магазина, о котором идет речь, записал видео с камер наблюдения на мобильный телефон и поделился этой записью в социальной сети. Подчеркивается, что на видеозаписи были запечатлены дети, и что противоправное разглашение такой информации представляет собой потенциально большой риск для их приватности.

## Штраф Grindr за передачу данных рекламодателям и недобросовестную модель монетизации



2021

### Intention to issue € 10 million fine to Grindr LLC

The Norwegian Data Protection Authority has notified Grindr LLC (Grindr) that we intend to issue an administrative fine of NOK 100 000 000 for not complying with the GDPR rules on consent.

- Our preliminary conclusion is that Grindr has shared user data to a number of third parties without legal basis, said Bjørn Erik Thon, Director-General of the Norwegian Data Protection Authority.

Grindr is a location-based social networking app for gay, bi, trans, and queer people. In 2020, [the Norwegian Consumer Council filed a complaint against Grindr](#) claiming unlawful sharing of personal data with third parties for marketing purposes. The data shared include GPS location, user profile data, and the fact that the user in question is on Grindr.

Our preliminary conclusion is that Grindr needs consent to share these personal data and that Grindr's consents were not valid. Additionally, we believe that the fact that someone is a Grindr user speaks to their sexual orientation, and therefore this constitutes special category data that merit particular protection.

**Кто:** Datatilsynet (Норвегия)

**Кого:** Grindr LLC

**Когда:** 2021.01

**За что:** нарушение ст. 5, 6 GDPR

**Как:** возможный штраф €10,000,000

**Причина:** приложение для знакомств Grindr, ориентированное на ЛГБТ-сообщество, обвиняется в грубых нарушениях GDPR в 2018-2020 годах, когда оно передавало данные пользователей крупным рекламодателям, в числе которых рекламная платформа MoPub, принадлежащая Twitter. MoPub, в свою очередь, мог делиться этими данными ещё со 100 компаниями-партнёрами. По оценкам Fortune, потенциальный штраф составляет треть предполагаемой чистой прибыли компании за этот период.

Одна из причин беспрецедентного штрафа — особая чувствительность данных (в т.ч. информация о сексуальной ориентации), которые передавал Grindr. В сочетании с информацией о местоположении сведения о сексуальной ориентации могли бы привести к преследованиям пользователей — например, в Катаре или Пакистане.

Надзорный орган не устроила и модель монетизации Grindr. Одно из преимуществ платной версии приложения — отсутствие таргетированной рекламы, и, как следствие, передачи данных о пользователе рекламодателям. Иначе говоря, пользователь мог гарантировать себе конфиденциальность только при покупке платной версии — что автоматически означает незаконность бесплатной.

## Штраф на контролера и процессора за недостаточные меры против взлома учетных записей на веб-сайте

# CNIL.

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL |   

### « Credential stuffing » : la CNIL sanctionne un responsable de traitement et son sous-traitant

27 janvier 2021

*La formation restreinte de la CNIL a récemment sanctionné de 150 000 euros et 75 000 euros un responsable de traitement et son sous-traitant pour ne pas avoir pris de mesures satisfaisantes pour faire face à des attaques par bourrage d'identifiants (credential stuffing) sur le site web du responsable de traitement.*

Entre juin 2018 et janvier 2020, la CNIL a reçu plusieurs dizaines de notifications de violations de données personnelles en lien avec un site internet à partir duquel plusieurs millions de clients effectuent régulièrement des achats. La CNIL a décidé de mener des contrôles auprès du responsable du traitement et de son sous-traitant, a qui était confié la gestion de ce site web.

Au cours de ses investigations, la CNIL a constaté que le site web en cause avait subi de nombreuses vagues d'attaques de type *credential stuffing*. Dans ce type d'attaque, une personne malveillante récupère des listes d'identifiants et de mots de passe « en clair » publiés sur Internet, généralement à la suite d'une violation de données. Partant du principe que les utilisateurs se servent souvent du même mot de passe et du même identifiant (l'adresse courriel) pour différents services, l'attaquant va, grâce à des « robots », tenter un grand nombre de connexions sur des sites. Lorsque l'authentification réussit, cela lui permet de prendre connaissance des informations associées aux comptes en question.

La CNIL a constaté que des attaquants ont ainsi pu prendre connaissance des informations suivantes : nom, prénom, adresse courriel et date de naissance des clients, mais également numéro et solde de leur carte de fidélité et des informations liées à leurs commandes.

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** неназванные компании

**Когда:** 2021.01


**За что:** нарушение ст. 32 GDPR

**Как:** штраф €150,000 на контролера и €75,000 на процессора

**Причина:** с 06.2018 по 01.2020 надзорный орган неоднократно получал жалобы от пользователей интернет-магазина о взломе их учетных записей. В то же время, владелец магазина и его технический подрядчик (процессор) решили сосредоточить свою стратегию реагирования на разработке инструмента для обнаружения и блокировки атак, запускаемых ботами. Однако на разработку этого инструмента ушел год с первых атак.

Надзорный орган подчеркнул, что контролер должен принять решение о реализации защитных мер и дать документированные инструкции своему подрядчику, подрядчик должен предлагать наиболее подходящие технические и организационные решения для обеспечения безопасности данных.

## Штраф за ненадлежащее правовое основание обработки данных заявителей на стимулирующие выплаты COVID-19



**Caso bonus Covid: il Garante privacy sanziona l'Inps per 300mila euro. Ok ai controlli, ma con modalità a prova di privacy**

Caso bonus Covid: il Garante privacy [sanziona l'Inps per 300mila euro](#)  
Ok ai controlli, ma con modalità a prova di privacy

Mancata definizione dei criteri per trattare i dati di determinate categorie di richiedenti il "bonus Covid", uso di informazioni non necessarie rispetto alle finalità di controllo, ricorso a dati non corretti o incompleti, inadeguata valutazione dei rischi per la privacy.

Con queste motivazioni, il Garante per la protezione dati personali ha ordinato all'Inps il pagamento di una sanzione di 300 mila euro in relazione alle violazioni commesse nell'ambito degli accertamenti antifrode effettuati dall'Istituto riguardo al "bonus Covid" per le partite Iva.

L'Istruttoria del Garante era stata avviata nel mese di agosto, in seguito a notizie di stampa, riguardo al trattamento, da parte dell'Istituto, dei dati dei richiedenti che ricoprono cariche politiche (nello specifico, incarichi di parlamentare o di amministratore regionale o locale).

Nel corso degli accertamenti l'Autorità, pur riconoscendo che lo svolgimento dei controlli sulla sussistenza dei requisiti previsti dalla legge per l'erogazione del bonus è riconducibile a compiti di interesse pubblico rilevante, ha riscontrato numerose criticità nelle modalità utilizzate dall'Istituto nei procedimenti.

L'Istruttoria dell'Autorità ha messo in luce che l'Inps non ha adeguatamente progettato il trattamento e non è stata in grado di dimostrare di aver svolto i controlli nel rispetto del Regolamento, violando i principi di privacy by design, di privacy by default e di accountability.

In primo luogo, dopo aver acquisito da fonti aperte i dati di decine di migliaia di persone che ricoprono incarichi di carattere politico, l'Istituto ha effettuato elaborazioni e incroci tra i dati di tutti coloro che avevano richiesto il bonus con quelli dei titolari dei predetti incarichi. Ciò senza però aver prima determinato se ai parlamentari e agli amministratori regionali o locali spettasse o meno tale beneficio, anche in considerazione delle differenti caratteristiche delle cariche ricoperte. In questo modo l'Inps ha violato i principi di liceità, correttezza e trasparenza stabiliti dal Regolamento Ue in materia di protezione dei dati personali.

L'Inps non ha rispettato neppure il principio di minimizzazione dei dati, avendo avviato i controlli finalizzati al recupero del bonus anche su tutti quei soggetti che, pur avendo richiesto, non lo avevano percepito, visto che la loro domanda era già stata respinta per ragioni indipendenti dalla carica ricoperta.

E' emerso inoltre che l'Inps non ha valutato adeguatamente i rischi collegati a un trattamento di dati così delicato come è quello riguardante i richiedenti un beneficio economico classificato come ammortizzatore sociale, non effettuando la valutazione di impatto sui diritti e la libertà degli interessati.

Per tali motivi, il Garante ha dichiarato illecito il trattamento dei dati personali effettuato dall'Inps e ha applicato la sanzione. L'Autorità ha inoltre prescrito all'Istituto di cancellare i dati non necessari fino ad ora trattati ed effettuare un'adeguata valutazione di impatto privacy.

Roma, 9 marzo 2021

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Управление государственной пенсионной системы Италии (Istituto Nazionale della Previdenza Sociale)

**Когда:** 2021.02

**За что:** нарушение ст. 5(1), 25, 35 GDPR

**Как:** штраф €300,000

**Причина:** Управление не определило надлежащее правовое основание для обработки определенных категорий данных, принадлежащих лицам, подавшим заявки на стимулирующие выплаты COVID-19. Кроме того, INPS не соблюдало принципы минимизации данных и неадекватно оценивало риски конфиденциальности, связанные со сбором данных.

## Штраф за уязвимости в использовании QR-кодов при проверке действительности разрешений на парковку



**Kto:** Garante per la protezione dei dati personali (Italia)

**Kogo:** муниципалитет Рима и оператор мобильной связи (Roma Servizi per La Mobilita Srl)

**Kогда:** 2021.02

**За что:** нарушение ст. 5, 6, 28, 32 GDPR

**Как:** штрафы €300,000 и €60,000 соответственно

**Причина:** надзорный орган обнаружил, что порядок использования QR-кодов для проверки действительности разрешений на парковку транспортных средств не обеспечивает достаточного уровня защиты данных, поскольку коды и личная информация, прикрепленная к ним, были общедоступны через приложения для мобильных устройств. Хотя основная ответственности лежит на муниципалитете Рима (как контролере), но оператор мобильной связи, будучи разработчиком системы использования QR-кодов и процессором данных, также был оштрафован за неправильную оценку рисков безопасности данных.

<https://www.garanteprivacy.it/garante/doc.jsp?ID=9562852>

<https://www.garanteprivacy.it/garante/doc.jsp?ID=9562831>

## Штраф за незаконную автоматическую пересылку электронной корреспонденции работника



**Datatilsynet**

Aktuelle nyheter 2021

### Får gebyr for ulovleg vidaresending av e-post

Ei verksemd har fått vedtak om gebyr på 250 000 kroner for ulovleg vidaresending av e-posten til ein tilsett. Namnet på verksemda er unntatt offentlegheit for å skjerme identiteten til de tilsette.



Bakgrunnen for saka er ein klage frå ein person som opplevde at arbeidsgjeveren tok i bruk automatisk vidaresending av e-post.

Arbeidsgjeveren bad arbeidstakaren sette på automatisk vidareending frå e-postkassa si til ei felles e-postkassa i verksemda. Dette skal ha blitt gjort av omsyn til drifta.

#### I strid med reglane

Etter å ha undersøkt saka konkluderer Datatilsynet med at verksemda mangla rettsleg grunnlag for vidareendinga. Den har skjedd i strid med reglane i forskrifta om arbeidsgjevarens innsyn i e-postkassa og anna elektronisk materiale, i tillegg til kravet om rettsleg grunnlag etter personvernforordninga.

**Kontaktperson**

Ida Småge Breidablikk  
Juridisk seniorrådgiver



Nummer: +47 22 39 89 70  
E-post: [ida@datatilsynet.no](mailto:ida@datatilsynet.no)

Publisert: 02.03.2021

**Кто:** Datatilsynet (Норвегия)

**Кого:** неназванная компания

**Когда:** 2021.03

**За что:** нарушение ст. 5, 6 GDPR

**Как:** возможный штраф €24,700

**Причина:** расследование было инициировано по жалобе работника, который узнал, что работодатель настроил автоматическую пересылку входящих сообщений из служебной на общий электронный почтовый ящик в компании. Это было сделано из соображений «повышения эффективности рабочего процесса».

DPA пришел к выводу, что у компании отсутствовали правовые оснований для такой пересылки. Также было выявлено отсутствие у контролера политики в отношении правил доступа к служебной электронной почте.

## Штраф за неведение о нарушении безопасности данных



PREZES  
URZĘDU OCHRONY  
DANYCH OSOBOWYCH

Wa

### DECYZJA

DKN.5131.7.2020

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeksu postępowania administracyjnego (Dz. U. z 2020 r. poz. 256 ze zm.), art. 7 ust. 1 oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000), art. 57 ust. 1 lit. a), art. 58 ust. 2 lit. i), art. 83 ust. 1 - 3 i art. 83 ust. 4 § 1 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 4.05.2016, str. 1 oraz Dz. Urz. UE L 119 z 4.05.2016, str. 2), zwanego dalej również „rozporządzeniem 2016/679”, po przeprowadzeniu postępowania administracyjnego w sprawie braku zgłoszenia naruszenia ochrony danych osobowych przez ENEA S.A. z siedzibą w Poznaniu, Prezes Urzędu Ochrony Danych Osobowych,

**stwierdzając naruszenie przez ENEA S.A. z siedzibą w Poznaniu, polegające na niezapowiedzeniu naruszenia bezpieczeństwa danych osobowych, na podstawie art. 33 ust. 1 rozporządzenia 2016/679, polegającego na niezapowiedzeniu naruszenia bezpieczeństwa danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin od momentu stwierdzenia naruszenia, nakłada na ENEA S.A. z siedzibą w Poznaniu**

**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** Enea

**Когда:** 2021.03

**За что:** нарушение ст. 33 и 34 GDPR

**Как:** штраф €29,700

**Причина:** неавторизованное лицо получило электронное письмо от работника Enea с незашифрованным и незащищенным паролем вложением, содержащим персональные данные нескольких сотен человек, тем самым нарушив конфиденциальность данных этих лиц. Хотя заинтересованные лица ранее просили Enea прояснить обстоятельства инцидента, предоставить его анализ и оценить, есть ли необходимость уведомить UODO и затронутых субъектов о нарушении безопасности данных, компания воздержалась от выполнения указанных действий.



# Штрафы за незаконный прямой маркетинг и нарушение правил передачи данных внутри группы компаний

1/97



- Procedimiento Nº: PS/00059/2020

## RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y con base en los siguientes

### ANTECEDENTES

**PRIMERO.** Desde el segundo trimestre del año 2018 se han recibido en esta Agencia 191 reclamaciones a la fecha del acuerdo de inicio 26/02/2020 (23 de las cuales entre el 1 de octubre de 2019 y febrero de 2020) contra la entidad VODAFONE ESPAÑA, S.A.U. (en lo sucesivo VODAFONE o VDF), con NIF A80907397, en las que se denuncia la realización de acciones de mercadotecnia y prospección comercial en nombre y por cuenta de VDF a través de llamadas telefónicas y mediante envío de comunicaciones comerciales electrónicas (mensajes SMS y correos electrónicos).

Tales acciones podrían vulnerar tanto la normativa Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en adelante LGT), la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante LSSICE), como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de Derechos Digitales (en adelante LOPDGD).

Lo anterior, porque estas comunicaciones electrónicas denunciadas se producen, por un lado y en lo que respecta a la LSSICE, sin que hayan sido solicitadas o expresamente autorizadas y/o sin atender el ejercicio del derecho a oponerse al envío de nuevas notificaciones; por otro, en cuanto a la LGT, sin facilitar la posibilidad de ejercer el derecho de oposición o bien, una vez que el afectado ha ejercido previamente su derecho de oposición a través de su inclusión en el fichero de exclusión publicitaria interno de las entidades indicadas (en adelante Listado Robinson Interno -LRI-), o a través del sistema general común de exclusión publicitaria denominado Listado Robinson Adigital -LRAD-; y, finalmente, por lo que respecta a la LOPDGD sin adecuar los procedimientos y garantías establecidas para la ejecución de acciones de mercadotecnia en el contenido de los contratos con los encargados de los tratamientos que actúan en nombre y por cuenta del responsable (VDF) y sin ofrecer al interesado los medios necesarios, suficientes y apropiados que le garanticen la protección de sus derechos y libertades.

Asimismo, debe ponerse de manifiesto que del análisis de las contestaciones a los requerimientos de información de esta Agencia evacuados por la entidad reclamada se desprende, en resumen, lo siguiente:

- No explican la razón por la que suceden y continúan sucediendo los hechos objeto de reclamación.
- No se indica el origen de los datos relativos al número de línea telefónica o dirección electrónica de los destinatarios.
- No se responde el motivo por el que hay reclamantes que han ejercido el derecho de oposición a recibir acciones de mercadotecnia y/o figuran en su LRI o LRAD y, sin embargo, se hayan realizado nuevamente acciones comerciales.

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Vodafone España, S.A.U.


**Когда:** 2021.03

**За что:** нарушение ст. 21, 28, 44 GDPR, ст. 23 LOPDGD, ст. 21 LSSI, ст. 48(1)(b) LGT


**Как:** штраф €8,150,000

**Причина:** причиной расследование в отношении компании было получение надзорным органом 191 жалобы на звонки и сообщения от имени Vodafone, «без запроса или прямого разрешения и/или без реализации компанией права субъектов на противодействие отправке новых уведомлений путем возражения». Оной из причин была несогласованность действий различных участников группы компаний Vodafone. Например, одна из компаний могла зафиксировать возражение субъекта на получение рекламных уведомлений, но не предоставить эту информацию другим участникам группы.

## Штрафы за нарушение безопасности данных и за несвоевременное уведомление об этом



agencia  
española  
protección  
datos



1/35

- Procedimiento Nº: PS/00179/2020

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

**PRIMERO:** Con fecha de 04/02/2019 la Directora de la Agencia Española de Protección de Datos acuerda iniciar actuaciones de investigación en relación a la notificación de una brecha de seguridad realizada por AIR EUROPA LÍNEAS AÉREAS, S.A., con CIF **\*\*\*CIF.1** (en lo sucesivo AIR EUROPA), relativa al acceso no autorizado a la información de contacto y tarjetas bancarias que afecta a 489.000 interesados y un volumen de 1.500.000 registros.

No obstante, en fecha 28/02/2020, se acordó abrir nuevas actuaciones de investigación a AIR EUROPA e incorporar a éstas la documentación que integraban las actuaciones previas del expediente E/02564/2019, que se declararon caducadas.

La notificación de brecha de seguridad se efectuó en fecha 28/11/2018 y el 22/01/2019 como notificación inicial y completa.

Posteriormente, el 22/01/2019 se efectuó otra notificación para corregir información aportada, según manifiesta AIR EUROPA, a discrepancias entre el acuse de recibo emitido por la sede electrónica de esta Agencia y los datos efectivamente introducidos en el formulario online. Las tres notificaciones contienen, entre otra, la siguiente información:

- Que en fecha 27/11/2018 se intentó en repetidas ocasiones notificar de manera inicial a esta Agencia a través del formulario habilitado al efecto en sede electrónica pero el procedimiento online de notificación imposibilitó la presentación por dicho medio, procediéndose a la presentación de manera inicial y presencial en fecha 28/11/2018.
- Responsable del tratamiento: AIR EUROPA cuyos datos se han incluido en el apartado de Entidades Investigadas.
- Fecha de detección de la brecha: **\*\*\*FECHA.1**
- Medios de detección de la brecha: AIR EUROPA recibe una notificación por parte del Banco Popular relativo a un potencial incidente de seguridad, lo que determina la activación del plan de respuestas ante incidentes por parte de AIR EUROPA, el día 17/10/2018.
- Fecha de inicio de la brecha: 12/05/2018
- Brecha resuelta a 17/11/2018.
- Justificación de la notificación tardía: N/A
- Resumen del incidente: el incidente de seguridad ha comportado el acceso no autorizado a información de tarjetas bancarias, numeración, fecha de

C/ Jorge Juan, 6  
28001 - Madrid

www.aepd.es  
sedeagpd.gob.es

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Air Europa Lineas Aereas, SA.

**Когда:** 2021.03

**За что:** нарушение ст. 32(1) и 33 GDPR

**Как:** штрафы €500,000 и 100,000

**Причина:** компания не предприняла необходимых технических и организационных мер для обеспечения надлежащего уровня безопасности данных своих клиентов, в результате чего произошел несанкционированный доступ к контактными данным и банковским счетам в отношении 489,000 человек и 1,500,000 записей данных. Кроме того, контролер уведомил AEPD о нарушении безопасности данных спустя 41 день, вместо положенных 72 часов.

## 811 Штраф за неназначение представителя в ЕС



**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** Locatfamily.com

**Когда:** 2021.03

**За что:** нарушение ст. 27 GDPR

**Как:** штраф €525,000

**Причина:** контролер не выполнил обязательство назначить в письменной форме представителя в ЕС и что DPA было получено 19 жалоб в связи с невыполнением компанией запросов на удаление данных и отсутствием представительства Locatfamily.com в ЕС.

**Предписание:** если контролер не назначит представителя в ЕС до 18.03.2021, он должен будет платить €20,000 штрафа за каждые две недели неисполнения предписания – до достижения максимальной суммы штрафа в €120,000.

## Штраф за незаконный прямой маркетинг и отсутствие необходимых мер безопасности данных



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Fastweb, S.p.a.


**Когда:** 2021.04

**За что:** нарушение ст. 5, 6, 7, 12, 13, 21, 24, 25, 32, 33(1), 34(1) GDPR


**Как:** штраф €4,501,868 и предписание привести обработку данных в соответствие с принципами GDPR

**Причина:** обработка персональных данных миллионов субъектов в целях телемаркетинга без их согласия. Расследование было инициировано в результате сотен сообщений и жалоб на непрерывные нежелательные телефонные звонки и интернет-услуги, предлагаемые Fastweb. Так, было обнаружено использование вымышленных номеров или номеров, не зарегистрированных в Реестре операторов связи (RCO), а также отсутствие адекватных мер безопасности для систем управления взаимоотношениями с клиентами.

## 813 Штраф за несоблюдение права быть забытым



1/13



**Procedimiento Nº: PS/00406/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes:

**ANTECEDENTES**

**PRIMERO:** Dña. A.A.A. (en adelante, la reclamante) con fecha 30 de julio de 2019 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra EQUIFAX IBERICA, S.L. con NIF B80855398 (en lo sucesivo, el reclamado o EQUIFAX). Los motivos en que basa la reclamación son que se han incluido sus datos en el fichero de solvencia patrimonial y de crédito Asnef-Equifax sin existir tal deuda y sin notificarla de que iba a ser incluida. Que una vez incluida en dicho fichero tampoco se la ha notificado.

Y, entre otra, aporta la siguiente documentación:

- Copia de carta dirigida a la reclamante y remitida por Testa Residencial Socimi, S.A. fechada a 20 de junio de 2019 donde consta:
  - o "Fecha de finalización del contrato": 02/08/2019
  - o "Relativo a": **\*\*\*DIRECCION.1**
  - o Consta, entre otro, el texto siguiente: *"...Aprovechamos la presente para recordarle que, según nuestros asientos contables, a día de hoy adeuda la suma de XXXX,XX € en concepto del impago de las rentas...."*
- Copia de carta dirigida a la reclamante y remitida por Testa Residencial Socimi, S.A. fechada a 10 de junio de 2019 donde:
  - o Consta, entre otro, el texto siguiente: *"Que en relación al contrato de arrendamiento número, **\*\*\*REFERENCIA.1** que tenemos con usted sobre el inmueble sito en **\*\*\*DIRECCION.1**, se ha detectado en nuestros asientos contables de "Testa Residencial Socimi, S.A." una deuda pendiente de XXXX,XX €. – euros, correspondientes al impago de los recibos de mayo del 2018 (deuda cedida por Building Center) julio de 2018 así como febrero, marzo, abril, mayo y junio de 2019 y consumos."*
- Copia de carta dirigida a Testa Residencial Socimi, S.A. y remitida por la reclamante donde consta:
  - o Que la presente carta es contestación de la recibida en fecha 13 de junio de 2019.
  - o Que la deuda del mes de mayo y julio 2018 no existe, pues la de mayo les fue realizada transferencia de los YYY€ que reclamaban, por el ayuntamiento de Gijón. Que se le envió a Testa el día 23 de marzo del 2019 copia del justificante de pago.
  - o Que respecto de la deuda del mes de julio 2018, no se les pasó recibo.
  - o Que respecto de los pagos de los meses de febrero, marzo, abril, mayo, junio, julio de 2019 se les pidió que usaran al Depósito de Garantía y la fianza para el pago.

C/ Jorge Juan, 6  
28001 – Madrid

www.aepd.es  
sede.aepd.gob.es

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Kutxabank SA

**Когда:** 2021.04

**За что:** нарушение ст. 17 GDPR

**Как:** штраф €100,000

**Причина:** контролер был обязан заблокировать данные клиента после получения его запроса на удаление, принимая технические и организационные меры для блокирования дальнейшей обработки персональных данных. В реальности, Kutxabank не смог своевременно выполнить запрос и потребовал от клиента подписать заявление об отказе от ранее направленного запроса на удаление, что позволило разблокировать клиентские данные. Испанский DPA отметил, что любой отказ субъекта от своих прав является ничтожным.

## 814 Штраф за публикацию персональных данных на веб-сайте



**Datatilsynet**

Lover og regler / Sentrale avgjørelser / 2021

### Gebyr til Asker kommune

Datatilsynet har gitt Asker kommune et overtredelsesgebyr på én million kroner. Gebyret gis etter at kommunen publiserte taushetsbelagte personopplysninger og fødselsnummer på hjemmesiden sin.



- Avvikene gjelder brudd på personopplysningsregelverkets krav om konfidensialitet, og omfatter både rutinesvikt og teknisk svikt. Personopplysninger som skulle vært skjermet er blitt gjort tilgjengelig for uvadkommende på kommunens hjemmeside, sier seksjonsleder Camilla Nervik.

#### Bakgrunn for saken

Kommunen ble varslet 19. mai 2020 av en privatperson om at dokumenttittel fra kommunens postlister inneholdt 127 navn og fødselsnummer i til sammen 170 journalposter. Opplysningene som var tilgjengelige var tittel på dokumentet, i tillegg til navn og fødselsnummer.

Flere av sakene gjaldt barn. I enkelte tilfeller har dette medført at også taushetsbelagte opplysninger er blitt offentliggjort, for eksempel i forbindelse med vedtak om PPT, spesialundervisning og boligtilskudd. Selve dokumentet har ikke vært offentlig tilgjengelig. Dokumenttittlene på de omtalte sakene ble umiddelbart fjernet fra kommunens nettsider.

#### Kontaktperson

Camilla Nervik  
seksjonssjef, seksjon for offentlige tjenester



Kontor: [\(+47\) 32 38 69 29](tel:+4732386929)  
E-post: [cau@datatilsynet.no](mailto:cau@datatilsynet.no)

Publisert: 09.04.2021

**Кто:** Datatilsynet (Норвегия)

**Кого:** муниципалитет Аскера


**Когда:** 2021.04

**За что:** нарушение ст. 5(1)(а), 6(1) GDPR

**Как:** возможный штраф €99,500

**Причина:** персональные данные 127 субъектов (включая нескольких несовершеннолетних) были опубликованы на веб-сайте муниципалитета без предварительной проверки и без наличия законного основания.

## Штраф за использование данных из общедоступных источников без надлежащего правового основания


1/184

• Procedimiento Nº: PS/00240/2019

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en consideración a los siguientes

ANTECEDENTES

**PRIMERO:** Se han recibido en la Agencia Española de Protección de Datos (AEPD) noventa y seis (96) reclamaciones contra EQUIFAX IBÉRICA, S.L., con NIF B80855398, (en adelante, la reclamada o EQUIFAX) por presunta vulneración de la normativa de protección de datos.

Las reclamaciones versan sobre el tratamiento de los datos personales de los reclamantes efectuado por EQUIFAX y materializado en su incorporación al Fichero de Reclamaciones Judiciales y Organismos Públicos (en lo sucesivo, FIJ) asociados a supuestas deudas en su mayoría contraídas, presuntamente, con Administraciones Públicas. Con carácter general, los datos personales objeto de tratamiento vinculados a presuntas deudas figuraron en documentos de las Administraciones Públicas, las entidades u organismos de Derecho Público dependientes de ellas o en resoluciones de los órganos jurisdiccionales que fueron publicados a través de boletines o diarios oficiales, mediante su inserción en los tablones de anuncios ubicados en la sede de las entidades u organismos o en el tablón edictal judicial único, con la finalidad de hacer efectiva la notificación de una resolución administrativa o judicial.

EQUIFAX IBÉRICA, S.L., con NIF B80855398, es la responsable del FIJ. Así lo ha reconocido en alguno de los documentos que obran en el expediente, como la carta que envió a los reclamantes número 36 (E/6174/2019), número 43 (E/11624/2019) y número 48 (E/2050/2020) para informarles de la inclusión de sus datos personales en el FIJ.

Cabe recordar, además, que la derogada Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD) regulaba en sus artículos 14 y 39 el Registro General de Protección de Datos, de consulta pública, que informaba de los tratamientos de datos, de las finalidades de esos tratamientos y de la identidad del responsable del tratamiento. En el citado Registro -actualizado a junio de 2016- EQUIFAX aparecía como responsable del FIJ, siendo la finalidad del fichero y los usos previstos la "prestación de servicios de solvencia patrimonial y crédito".

Si bien en el acuerdo de apertura y en la propuesta de resolución se indicó que eran 97 las reclamaciones formuladas contra EQUIFAX, y así consta en la relación de reclamantes que figura en el Anexo I y en la descripción de las reclamaciones (Antecedente Primero), son realmente 96 reclamaciones las que integran este expediente, habida cuenta de que el reclamante 3 y el 27 son la misma persona que ha presentado en dos momentos distintos diferente documentación anexa.

Tomando en consideración que no debemos efectuar ninguna rectificación en el Antecedente Segundo, por cuanto dicho Antecedente se incorporó a la relación de hechos probados como Hecho Probado Primero, no se altera su contenido, que

C/ Jorge Juan, 6  
28001 - Madrid

www.aepd.es  
sede.aepd.gob.es

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Equifax Ibérica, SL

**Когда:** 2021.04

**За что:** нарушение ст. 5(1), 6(1), 14 GDPR

**Как:** штраф €1,000,000

**Причина:** контролер был оштрафован по результатам расследования, начатого после поступления 96 жалоб субъектов на сбор из общедоступных источников (публикаций в документах государственных органов, информационных бюллетенях или газетах) и использование персональных данных об их предполагаемых долгах без согласия этих субъектов.

Контролер также не предоставил субъектам информацию об обработке их персональных данных, хотя эти данные не были получены от самих субъектов данных. Кроме того, законный интерес компании Equifax не может быть использован в качестве действительного правового основания для рассматриваемой обработки персональных данных.

## Штраф за незаконную обработку данных работников для мониторинга, оценки и дисциплинарных взысканий

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Proma S.S.A. Srl.

**Когда:** 2021.04

**За что:** нарушение ст. 5, 13 GDPR

**Как:** штраф €40,000

**Причина:** DPA провел проверку деятельности контролера по обращению от лица 11 работников и установил, что система управления производственным процессом и контроля безопасности труда требовала регистрации работников при начале работы на станках и собирала персональные данные сверх минимально обусловленных целью. Несмотря на заверения компании, что данные агрегировались и не использовались для мониторинга, оценки работников и дисциплинарных взысканий:

- идентификация работников работодателем была возможна с использованием дополнительных данных;
- работодатель все же использовал данные для расследований и дисциплинарных взысканий, не сообщал работникам обо всем объеме собираемых данных, полном списке целей и оснований обработки, сроках хранения.



G P D P

**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

**Ordinanza ingiunzione nei confronti di Proma S.S.A. s.r.l. -  
15 aprile 2021 [9586936]**

VEDI ANCHE [Newsletter del 19 maggio 2021](#)  
[doc. web n. 9586936]

Ordinanza ingiunzione nei confronti di Proma S.S.A. s.r.l. - 15 aprile 2021

Registro dei provvedimenti  
n. 136 del 15 aprile 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzone, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale:

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito, "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTO il reclamo presentato al Garante ai sensi dell'articolo 77 del Regolamento nei confronti di Proma S.S.A. s.r.l.;

ESAMINATA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Agostino Ghiglia;

PREMESSO

**1. Il reclamo nei confronti della società e l'attività istruttoria.**

1.1. Con reclamo dell'11 febbraio 2019, presentato da Fiom Cgil Molise su mandato di undici lavoratori, sono state lamentate presunte violazioni della disciplina posta in materia di protezione dei dati personali in relazione all'utilizzo da parte di Proma S.S.A. s.r.l. (di seguito, la società), nell'unità produttiva di Pozzilli (Isernia), del sistema informatico PPMS (Proma Productivity Management System).

In particolare con il reclamo è stato lamentato che la società, in relazione all'attivazione del sistema PPMS - oggetto di autorizzazione da parte dell'ispettorato territoriale del lavoro di Campobasso-Isernia in data 9 luglio 2018 ed attivo dal 1° agosto 2018 - "sta obbligando tutti i



## Штраф за вторичное использование чувствительных данных пациента без его согласия



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** физическое лицо (врач)

**Когда:** 2021.04


**За что:** нарушение ст. 5, 6, 9 GDPR

**Как:** штраф €5,000

**Причина:** Врач использовала скачанные из архива больницы данные о здоровье пациента и фотографии с его операции в своей презентации на международной конференции, а также в составе заявки на конкурс «Лучший клинический случай 2017 года». Ее работа выиграла, и данные пациента были опубликованы на сайте хирургического общества в следующем составе: инициалы пациента, возраст, пол, подробный анамнез перенесенной патологии, подробности госпитализаций с 1980 по 2016 год, и операций, перенесенных в этот период с указанием дат, 14 диагностических изображений, а также 22 фотографии, изображающие субъекта персональных данных во время операции.

Пациент ранее дал больнице согласие на «эпидемиологическое и научное исследование». Врач же заявила, что вместо имени пациента она указала его инициалы, и это, по ее мнению, сделало данные анонимными.

## Штраф за не проверку полномочий предполагаемых представителей субъектов


1/138

• Procedimiento N°: PS/00236/2020

**RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR**

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

**ANTECEDENTES**

**PRIMERO:** Ante esta Agencia se han venido presentando diversas reclamaciones contra la entidad EDP ENERGÍA, S.A.U. en las que sustancialmente se denuncia el tratamiento de datos personales sin consentimiento del interesado. Dichos tratamientos se producen en el marco de la contratación de servicios de electricidad efectuadas supuestamente por un representante del cliente, sin que dicha entidad pueda acreditar la existencia de tal representación y han dado lugar a diversas actuaciones de esta Agencia, entre las que cabe mencionar la incoación de diversos procedimientos sancionadores como los procedimientos PS/00101/2018, PS/00363/2018 o PS/00109/2019, que han concluido declarando la existencia de una infracción de lo previsto en la normativa de protección de datos.

**SEGUNDO:** A la vista de los antecedentes mencionados en el número anterior, el día 3 de junio de 2019 la Directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos el inicio de actuaciones previas de investigación a fin de acreditar, en su caso, la existencia de una conducta regular y continuada de posible vulneración de la normativa de protección de datos por parte de EDP ENERGÍA, S.A.U.

**TERCERO:** Con fecha de 13 de junio de 2019 se presentó ante la AEPD una reclamación contra EDP ENERGÍA S.A.U. por el tratamiento de datos personales sin consentimiento del interesado en la contratación del suministro de energía eléctrica. Dicha reclamación formulada por Doña **A.A.A.**, viene referida a la contratación de suministro de energía eléctrica con la sociedad EDP ENERGÍA, S.A.U. realizada el 9 de enero de 2019 a nombre de la reclamante sin su consentimiento. La reclamación fue admitida a trámite mediante acuerdo de la Directora de la Agencia de Protección de datos con fecha 10 de septiembre de 2019.

**CUARTO:** El día 17 de diciembre de 2019, la Subdirección General de Inspección formula requerimiento a EDP ENERGÍA, S.A.U. para que facilite la siguiente información:

1. Especificación de los canales de contratación (telefonía, internet, distribuidores propios o subcontratas, fuerza de ventas con visitas a domicilio propia o subcontratada, etc....) de los servicios comercializados por EDP ENERGÍA, S.A.U. a personas físicas.
2. Descripción del procedimiento de contratación seguido a través de cada uno de los canales anteriores cuando la contratación es realizada por un tercero en

© Jorge Juan, 8  
28001 - Madrid

www.aepd.es  
info@aedp.gob.es

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** EDP Energía, S.A.U.

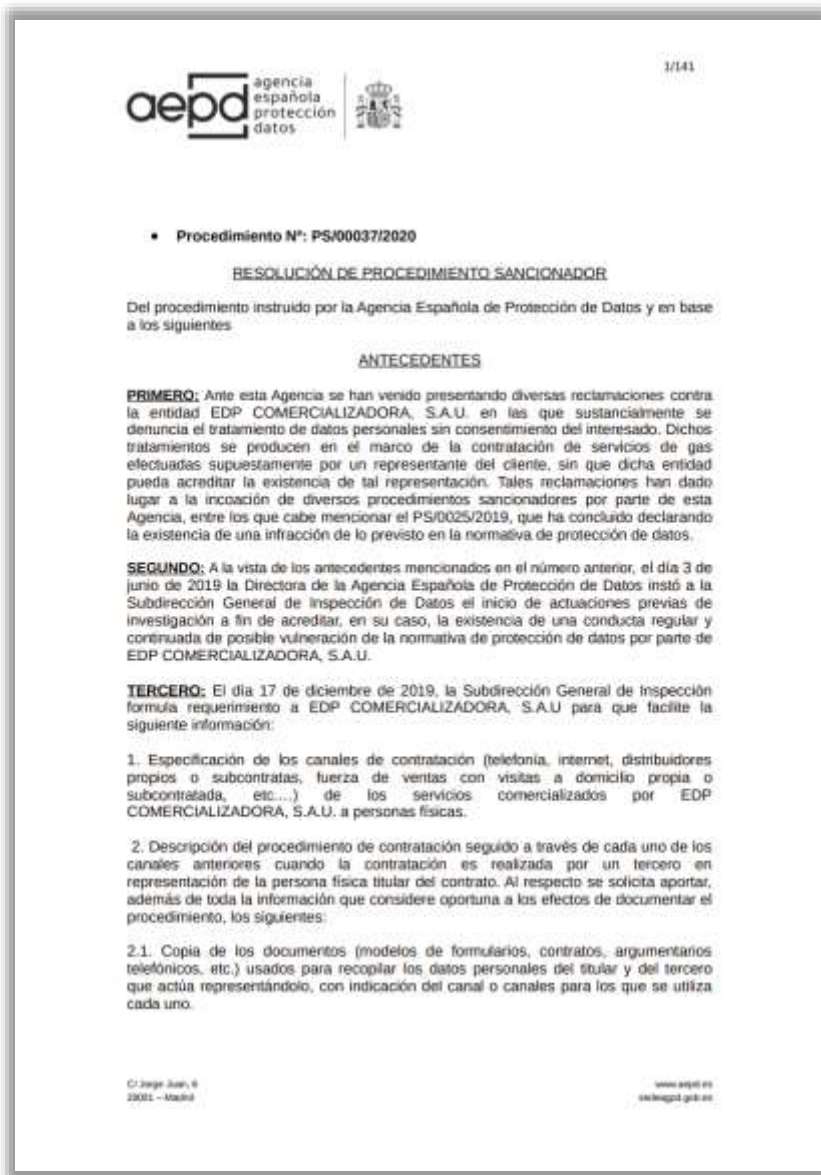
**Когда:** 2021.05

**За что:** нарушение ст. 13, 25 GDPR

**Как:** штрафы €1,000,000 (ст.13) и €500,000 (ст.25)

**Причина:** контролер направлял субъектам ненадлежащее уведомление о конфиденциальности при сборе их данных – субъекты не получали информацию об их правах по ст. 15-22 GDPR, а контактные данные контролера (например, его адрес) оказались неполными. Кроме того, деловая практика компании позволяла заключать контракты с представителями клиентов, однако в этих случаях контролер не проверял правомерность получения данных клиентов и не осуществлял проверку полномочий предполагаемых представителей.

## Штраф за непроверку полномочий предполагаемых представителей субъектов



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** EDP Comercializadora, S.A.U.

**Когда:** 2021.05

**За что:** нарушение ст. 13, 25 GDPR

**Как:** штрафы €1,000,000 (ст.13) и €500,000 (ст.25)

**Причина:** компания не реализовала технические и организационные меры безопасности для защиты данных физических лиц, заключивших договор газовых услуг через посредников (представителей), так как не существовало процедуры проверки полномочий представителя, что подвергало субъектов рискам, включая кражу или экономический и другой ущерб. Кроме того, субъектов часто просили дать согласие на получение предложений, связанных с услугами компании, без доказательства того, что третьи стороны, запрашивающие такое согласие, были уполномочены контролером для такой обработки данных.

## Штраф за уведомление о нарушении безопасности персональных данных

**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** Партия Свободы («PVV»)

**Когда:** 2021.05

**За что:** нарушение ст. 33 GDPR

**Как:** штраф €7,500

**Причина:** 11.01.2019 надзорный орган получил жалобу, в которой говорилось, что 10.01.2019 PVV отправила электронное письмо группе из 101 получателя, включая заявителя, содержащее персональные данные, включая сведения о политических взглядах субъектов (получателей письма) и их адресах электронной почты, которые были видны в списке рассылки электронного письма.



AUTORITEIT  
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens  
Postbus 93374, 2509 AJ Den Haag  
Bezuidenhoutseweg 30, 2594 AV Den Haag  
T 070 888 500 - F 070 888 501  
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Beveiligd

Stichting Ondersteuning Provinciale  
Fractie Overijssel Partij voor de Vrijheid  
[VERTROUWELIJK]  
Steenmeijerstraat 57  
7555 NV HENGLO

Datum  
16 juni 2020

Ons kenmerk  
[VERTROUWELIJK]

Contactpersoon  
[VERTROUWELIJK]

Onderwerp  
Besluit tot het opleggen van een bestuurlijke boete

Geachte [VERTROUWELIJK],

De Autoriteit Persoonsgegevens (hierna: AP) heeft besloten aan de Stichting Ondersteuning Provinciale Fractie Overijssel Partij voor de Vrijheid (PVV) (hierna: PVV Overijssel) een bestuurlijke boete van € 7.500,- -- op te leggen. De AP is van oordeel dat de PVV Overijssel in de periode van 14 januari 2019 tot heden heeft nagelaten oen inbreuk in verband met persoonsgegevens, zolang onredelijke vertraging en uiterlijk binnen 72 uur naad de PVV Overijssel op 11 januari 2019 op de hoogte raakte van de inbreuk, te melden aan de AP. De PVV Overijssel heeft daarmee artikel 33, eerste lid, van de Algemene Verordening Gegevensbescherming (hierna: AVG) overtreden.

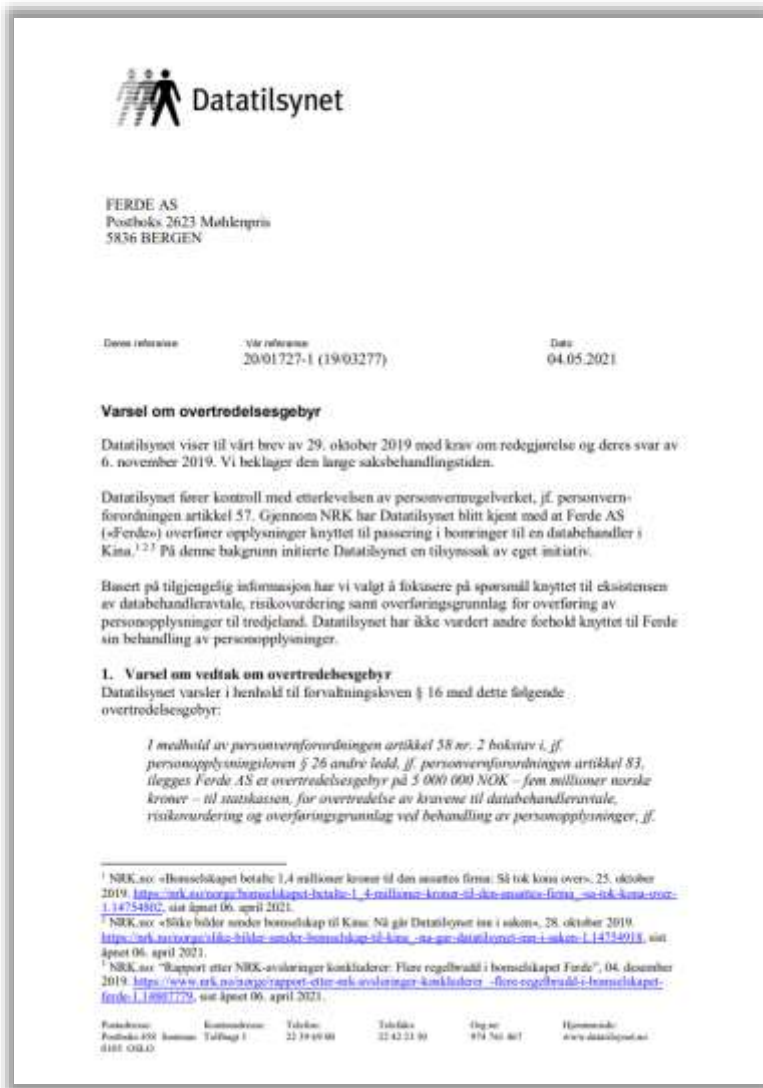
Hierna wordt het besluit toegelicht. Hoofdstuk 1 bevat de relevante feiten en het procesverloop. In hoofdstuk 2 wordt het wettelijk kader beschreven. In hoofdstuk 3 volgt de beoordeling van de AP, waarna in hoofdstuk 4 de hoogte van de bestuurlijke boete wordt gemotiveerd. Tenzlotte bevat hoofdstuk 5 het dictum en de rechtsmiddelenclausule.

**1. Feiten en procesverloop**

Stichting Ondersteuning Provinciale Fractie Overijssel Partij voor de Vrijheid (PVV) is statutair gevestigd aan de Steenmeijerstraat 57, 7555 NV te Hengelo. De stichting heeft onder meer het verlenen van bestuurlijke en administratieve assistentie aan de Fractie (zoals bedoeld in artikel 5 van het reglement van orde voor de vergadering en andere werkzaamheden van de Provinciale Staten van Overijssel of een

1

## Штраф за незаконную трансграничную передачу персональных данных автомобилистов в Китай



**Кто:** Datatilsynet (Норвегия)

**Кого:** Ferde AS

**Когда:** 2021.05

**За что:** нарушение ст. 28(3), 32, 44 GDPR

**Как:** возможный штраф €498,000

**Причина:** Норвежская компания по управлению местными платными дорогами Ferde AS использовала технологию распознавания номерных знаков машин, чтобы контролировать оплату проезда. Норвежский регуляторный орган прочитал в новостях, что компания использует для этого процессора, который находится в Китае. В ходе расследования было установлено, что услугами подрядчика Ferde пользовались с 2017 года, но к мерам по соответствию GDPR прибегли только в период с 2018 по 2019 год. Номерные знаки регулятор посчитал персональными данными. Камеры передавали только фото номеров, а фотографии водителей в кадр не попадали.

Ferde AS использовал сервис с сентября 2017 целый год перед тем, как подписать Data Processing Agreement с китайским подрядчиком в сентябре 2018 года. Для передачи персональных данных в Китай Ferde подписали SCC, но только в 2019 году. В период с 2017 по 2019 год передача данных никоим образом не регулировалась. Как и в случае с предыдущими пунктами, формальную оценку рисков провели только в апреле 2019 года. Оценка показала, что передача данных в Китай – низкорисковая активность.

# Штраф за нарушение безопасности персональных данных 3,2 млн. субъектов



NORGES IDRETTSFORBUND OG OLYMPISKE OG  
PARALYMPISKE KOMITÉ  
Postboks 5000  
0840 OSLO

*Unntatt offentlighet:*  
*Offl. § 13 jf. Popplyl. § 24 (1) 2.*  
*pkt.*

Deres referanse	Vår referanse	Dato
	20/01626-7	05.05.2021

## Vedtak om overtredelsesgebyr - Brudd på personopplysningsikkerheten - NORGES IDRETTSFORBUND OG OLYMPISKE OG PARALYMPISKE KOMITÉ

Vi viser til vårt varsel om vedtak om overtredelsesgebyr datert 2. desember 2020, og merknader til dette i brev fra Norges idrettsforbund og olympiske og paralympiske komité (heretter NIF) datert 22. desember 2020.

Dere skriver at NIF er enig i de faktiske forholdene i saken, men at NIF prinsipielt mener at overtredelsesgebyr ikke burde vært ilagt, og subsidiært at det varslede overtredelsesgebyret er vesentlig for høyt. Disse merknadene behandles i vedtakets punkt 5.

### 1. Vedtak om overtredelsesgebyr

Datatilsynet fatter følgende vedtak:

1. Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i pålegges Norges idrettsforbund og olympiske og paralympiske komité, org.nr. 947 975 072, å betale et overtredelsesgebyr til statskassen på 1 250 000 – en million to hundre og femti tusen – kroner for brudd på personvernforordningen artikkel 5 nr. 1 bokstav a, c og f, artikkel 6 og artikkel 32.

Informasjon om klagerett fremgår i vedtakets punkt 6.

### 2. Nærmere om sakens faktiske forhold

Nedenfor vil vi gjengi faktum i saken slik det samlet fremgår av avviksmeldingen, NIFs svar på krav om redegjørelse 28. februar 2020, Skype-møte med Datatilsynet 4. mai 2020, NIFs svar på krav om ny redegjørelse 25. mai 2020, rapporten fra Orange Cyberdefense av 3. juni 2020 og merknadene til Datatilsynets varsel datert 22. desember 2020.

### NIF som organisasjon

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr.:	Hjemmeside:
Postboks 458 Sentrum	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no
0105 OSLO					

**Kto:** Datatilsynet (Norge)

**Kogo:** Норвежский Олимпийский и Паралимпийский комитет и Конфедерация спорта (NIF)

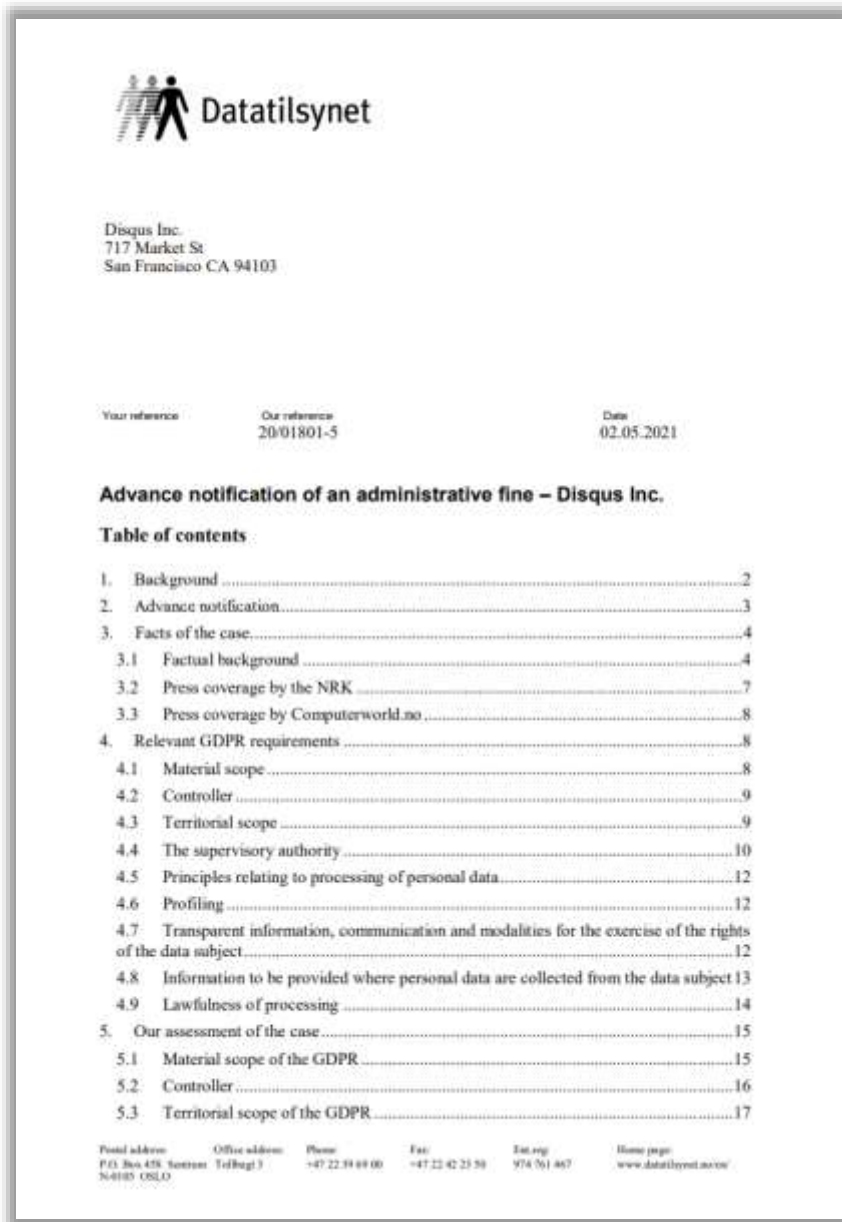
**Kогда:** 2021.05

**За что:** нарушение ст. 5, 6, 32 GDPR

**Как:** штраф €124,400 (первоначальный размер штрафа €249,300 был уменьшен после оценки финансового состояния контролера)

**Причина:** раскрытие персональных данных (имена, даты рождения, адреса, номера телефонов и адреса электронной почты) 3,2 млн. человек онлайн в течение 87 дней после ошибки, возникшей при тестировании облачного решения. Среди пострадавших 486,447 были детьми в возрасте от 3 до 17 лет. DPA подчеркнул, что тестирование могло проводиться путем обработки синтетических данных или с использованием меньшего количества персональных данных.

## Экстерриториальный штраф калифорнийской компании за нарушение безопасности персональных данных



**Кто:** Datatilsynet (Норвегия)

**Кого:** Disqus Inc. (США)

**Когда:** 2021.05

**За что:** нарушение ст. Art. 5(1), 5(2), 6, 12, 13 GDPR

**Как:** возможный штраф €2,500,000

**Причина:** незаконное раскрытие посредством веб-виджета персональных данных контролером в адрес своих партнеров по рекламной деятельности.

## Штраф за непроверку источников персональных данных для телемаркетинга



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Iren Mercato S.p.A.

**Когда:** 2021.05

**За что:** нарушение ст. 5(1) и (2), 6(1), 7(1) GDPR

**Как:** штраф €2,856,169

**Причина:** контролер использовал персональные данные для телемаркетинга, которые он не собирал напрямую, а получил из других источников. Компания не проверяла, были ли получены действительные согласия от адресатов рекламы на обработку их данных. Контролер получил персональные данные от своего поставщика, который получил данные от двух других компаний.



## Штраф за невыполнение субпроцессором требований к безопасности сведений о состоянии здоровья



**Кто:** Integritetsskyddsmyndigheten (Швеция)

**Кого:** MedHelp AB

**Когда:** 2021.06

**За что:** нарушение ст. 5, 6, 9, 13, 32 GDPR

**Как:** штраф €1,200,000

**Причина:** в Швеции работает управляемая компанией Inera горячая линия 1177, где можно получить консультации по различным вопросам, связанным со здоровьем. Компания Medhelp AB была привлечена для обработки поступающих звонков в некоторых регионах страны. Medhelp, в свою очередь, заключила контракт с компанией Medcall Co Ltd (Таиланд) на прием звонков по выходным и в ночное время. И Medhelp, и Medcall заключили контракт с технологической компанией Voice Integrate Nordic AB на ведение записи разговоров.

В 2019 году у Voice Integrate произошла утечка записей звонков из-за неправильной настройки подключенного к сети сервера, который был общедоступным через Интернет и не был защищено шифрованием. DPA посчитал, что MedHelp не приняла надлежащих технических и организационных мер для обеспечения надлежащего уровня безопасности данных. Кроме того, поручение обработки персональных данных компании Medcall является неправомерным, так как иностранная компания не подпадает под действие шведского законодательства о соблюдении медицинской тайны.

## Условный срок и штрафы за нарушения информационной приватности работников и слежку за ними

BBC NEWS | РУССКАЯ СЛУЖБА

Главная Коронавирус Истории Видео Фильмы Подкасты

### "Массовая слежка". IKEA во Франции оштрафована на 1 млн евро за сбор данных о сотрудниках

15 июня 2021



Суд оштрафовал французское подразделение компании IKEA на миллион евро за незаконный сбор личных данных сотрудников. Его бывший глава Жан-Луи Байо приговорен к двум годам заключения условно и оштрафован на 50 тыс. евро.

По словам прокурора Памелы Табардел, жертвами незаконного сбора данных стали около 400 сотрудников магазинов IKEA во Франции в 2009-2012 годах. "Речь идет о защите нашей частной жизни от угрозы массовой слежки," - заявила она в марте, когда процесс начался.

**Кто:** Cour d'appel de Versailles (Франция)

**Кого:** IKEA France

**Когда:** 2021.06

**Как:** штраф компании €1,000,000; бывший глава компании во Франции Жан-Луи Байо приговорен к двум годам заключения условно и оштрафован на €50,000; отвечавший за управление рисками Жан-Франсуа Пэрис приговорен к 18 месяцам заключения условно и оштрафован на €10,000

**Причина:** противоправный сбор данных о 400 работниках магазинов IKEA во Франции в 2009-2012 годах. IKEA пользовалась услугами частной компании Eirpase, которая в свою очередь получала личные данные от работников полиции. IKEA France интересовала информация о стиле жизни работников и их прошлых нарушениях закона. Однако некоторые менеджеры пользовались для получения информации и личными связями в полиции.

## 827 Штраф за неизбирательное наблюдение за работниками



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** муниципалитет Больцано

**Когда:** 2021.06

**За что:** нарушение ст. 5(1)(a) и (c), 6, 9,13, 35, 88 GDPR

**Как:** штраф €84,000

**Причина:** муниципалитет в течение примерно десяти лет использовал средства контроля и мониторинга для слежения за действиями своих работников в сети Интернет. Получаемые данные хранились в течение одного месяца в виде специальных отчетов для целей сетевой безопасности. Муниципалитет не смог должным образом проинформировать работников о системе мониторинга и провел превентивный и обобщенный сбор данных, касающихся подключений к веб-сайтам, посещаемых отдельными работниками, что несоразмерно цели обработки.

Кроме того, были обнаружены нарушения в работе службы психологической помощи муниципалитета. В частности, используемая работниками типовая форма «Запрос на внеочередное медицинское обследование» должна была также визироваться руководителем работника, что представляет собой незаконную обработку данных о состоянии здоровья.

## Штраф за неправильно спроектированное приложение для whistleblowing



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Aeroporto Guglielmo Marconi di Bologna S.p.a.

**Когда:** 2021.06

**За что:** нарушение ст. 5(1)(f), 25(1), 32 и 35 GDPR

**Как:** штраф €40,000

**Причина:** Аэропорт использовал приложение для организации сбора и управления заявками о незаконных действиях своих работников и других заинтересованных лиц (whistleblowing). Приложение "WB confidential" использовалось через поставщика SaaS, который выступал в качестве процессора. Предоставляемые заявки содержали идентификационные данные информатора, информацию, относящуюся к заявке, и любую прилагаемую документацию. Однако, из-за ограниченного количества обработанных заявок и данных, контролер решил не проводить DPIA.

Из-за «малого использования» информации и «крайне низкой вероятности угроз» контролер решил не шифровать персональные данные, хранящиеся в его базе данных, и передавал их через общедоступные сети. Контролер решил, что шифрование нужно только в случаях обработки больших объемов данных, а реализация такой функции потребовала покупки дополнительного софта с непропорционально высокими затратами на реализацию. Кроме того, технический доступ был оставлен только для процессора, который не был заинтересован в передаче или распространении каких-либо данных.

## Штраф за нарушения при обработке отпечатков пальцев клиентов и работников

Valstybinė duomenų apsaugos inspekcija

### Sporto klubui skirta bauda už Bendrojo apsaugos reglamento pažeidimus tvarkant darbuotojų pirštų atspaudus

Tituolis • Naujienos • Sporto klubui skirta bauda už Bendrojo duomenų apsaugos reglamento pažeidimus tvarkant klientų ir darbuotojų pirštų atspaudus

Data: 2021.06.21 | Vertinimas: 13

**#BDAR BAUDA**

Valstybinė duomenų apsaugos inspekcija (VDAI) anksčiau tyrė dėl biometrinių asmenų duomenų tvarkymo sporto klube ir už nustatytus Bendrojo duomenų apsaugos reglamento (BDAR) pažeidimus skyrė 20 tūkst. Eur baudą UAB „VS FITNESS“. Bauda skirta už BDAR 5 straipsnio 1 dalies a ir c punktų, 9 straipsnio 1 dalies, 13 straipsnio 1-2 dalies, 30 straipsnio, 35 straipsnio 1 dalies nuostatų pažeidimus, t. y. už biometrinių duomenų tvarkymą, neturint savanoriško duomenų subjekto sutikimo, taip pat neužtikrinimą kiti galiojančiam žiniatinkliui keliamų reikalavimų. Duomenų subjekto teisės būti informuotiems apie duomenų tvarkymą netinkamai įgyvendinimą, taip pat nustatyta, kad bendrovė nebuvo atlikusi biometrinių duomenų tvarkymo poveikio duomenų apsaugai vertinimo, neturėdama veiklos planų.

**Кто:** Valstybinei duomenų apsaugos inspekcijai (Литва)

**Кого:** UAB VS „Fitness“

**Когда:** 2021.06

**За что:** нарушение ст. 5, 9, 13, 30, 35 GDPR

**Как:** штраф €20,000

**Причина:** согласно расследованию, проведенному по жалобе субъекта, спортклуб:

- сканировал отпечатки пальцев для предоставления услуг, не предлагая альтернативного способа идентификации;
- собирал недобровольное согласие с субъектов данных;
- ненадлежащим образом информировал об обработке;
- не выполнял DPIA;
- не вел RoPA;
- при обработке отпечатков работников полагался на согласие, не указывая цель и правовое основание, а также без информирования и DPIA.

На размер штрафа повлияли отягчающие обстоятельства виде обработки специальных категорий персональных данных без оснований и нарушение принципа прозрачности, а также финансовое состояние спортклуба и ограничения работы из-за коронавируса.

## Штраф за использование алгоритмов при оценке успеваемости доставщиков



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Foodinho s.r.l. (материнскую компанию GlovoApp)

**Когда:** 2021.06

**За что:** нарушение ст. 5(1) а), с), е), 13, 22(3), 25, 30(1) а), б), с), ф), г), 32, 35, 37(7) GDPR

**Как:** штраф €2,600,000

**Причина:** на основании истории доставок, а также отзывов пользователей и бизнес-партнёров (ресторанов), система формирует индивидуальный рейтинг доставщика. Полученная оценка помогает распределить заказы на платформе и может лишить возможности принимать заказы самых неблагонадёжных. Сами подрядчики не были уведомлены о том, что в Glovo работает такая система. Более того, компания не провела проверку алгоритмов на их статистическую точность и недискриминацию, а также не предоставила доставщикам возможность оспорить результаты профилирования.

Таже были выявлены такие нарушения как неназначение DPO (ст.37), отсутствие ROPA (ст.30), нехватка мер информационной безопасности (ст.32).

## 831 Штраф за тестирование облака на реальных персональных данных



### Norwegian Confederation of Sport fined for inadequate testing

The Norwegian Data Protection Authority has fined the Norwegian Confederation of Sport (NIF) EUR 125,000 (NOK 1,250,000) for a GDPR violation. The backdrop for this case is that personal data about 3.2 million Norwegians was available online for 87 days as a result of an error in connection with testing of a cloud computing solution.

The Data Protection Authority finds that NIF had failed to establish satisfactory security measures for the testing, and that testing with such a large quantity of personal data was not necessary.

#### Background

This case started when NIF submitted a discrepancy report to the Data Protection Authority on 20 December 2019, in response to an alert from the Norwegian National Cyber Security Centre (NCSC) that the personal data was available on a public IP address. The discrepancy occurred when they were testing solutions for moving a database from a physical server environment to the cloud.

**Кто:** Datatilsynet (Норвегия)

**Кого:** Norges idrettsforbund (Норвежская конфедерация спорта)

**Когда:** 2021.06

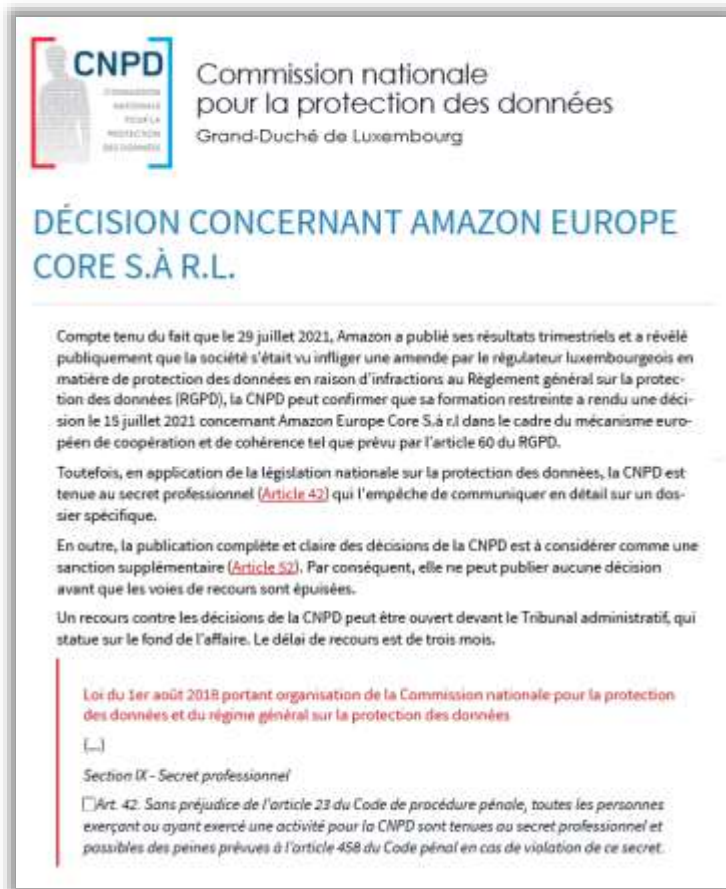
**За что:** нарушение ст. 5(1) f), 32 GDPR

**Как:** штраф €125,000

**Причина:** в 2019 году норвежская конфедерация спорта с базой данных в 3,2 миллиона человек проводила перенос своих систем из физических серверов в облако. Чтобы протестировать решение облачного провайдера, организация решила закинуть в облако сразу всю базу и посмотреть что будет. Помимо прочего, в базе находились данные 486 тысяч детей. Через некоторое время норвежский национальный центр кибербезопасности (National Cyber Security Center) уведомил норвежский надзорный орган, что нашёл персональные данные в тестируемом облаке в открытом доступе через публичный IP-адрес.

Перед внедрением облачных серверов организация не провела оценку рисков безопасности, что нарушает принцип целостности и конфиденциальности, а также требования к информационной безопасности. Использование реальных персональных данных для тестирования решения не имело законного основания.

## 832 Оборотный штраф на Amazon Europe Core в €746 млн.



**Кто:** Commission nationale pour la protection des données (Люксембург)

**Кого:** Amazon Europe Core S.à.r.l.

**Когда:** 2021.07

**За что:** нарушение ст. 6(1), 12, 13, 14, 15, 16, 17, 21 GDPR

**Как:** штраф €746,000,000 и предписание об исправлении нарушений в течение 6 месяцев (дополнительный штраф в €746,000 за каждый день просрочки)

**Причина:** Amazon собирает данные о продавцах, покупателях на сайте и пользователей виртуального помощника Alexa. Компания заявляет, что данные нужны для улучшения качества обслуживания клиентов, и устанавливает правила для использования данных работниками. Amazon считает решение CNPD безосновательным и намерена подать апелляцию.

**Предписание:**

- обеспечить легальность обработки данных для целей таргетированной рекламы (ст.6 GDPR);
- обеспечить выполнение обязанностей по раскрытию пользователям информации (ст. 12, 13 и 14 GDPR);
- выполнять обязанности по рассмотрению требований субъектов о предоставлении доступа к данным, а также об их уточнении или уничтожении (ст. 15-17 GDPR);
- обеспечить субъектам возможность выражать несогласие с обработкой персональных данных, включая любую обработку, связанную с привлечением клиентов (ст.21 GDPR).





AUTORITEIT  
PERSOONSgegevens

# Boete TikTok vanwege schenden privacy kinderen

Persbericht / 22 juli 2021

De Autoriteit Persoonsgegevens (AP) heeft videoapp TikTok een boete van 750.000 euro opgelegd wegens het schenden van de privacy van jonge kinderen. De informatie die de Nederlandse gebruikers – veelal jonge kinderen – van TikTok kregen bij het installeren en gebruiken van de app, was in het Engels en daardoor niet goed te begrijpen. Door de privacyverklaring niet in het Nederlands aan te bieden legde TikTok onvoldoende uit hoe de app persoonsgegevens verzamelt, verwerkt en verder gebruikt. Dat is in strijd met de privacywetgeving, waar het uitgangspunt is dat altijd duidelijk moet zijn wat er met je persoonsgegevens gebeurt.

In Nederland hebben veel kinderen TikTok op hun telefoon staan. De AP startte vorig jaar een uitgebreid onderzoek naar de app, omdat er zorgen waren over de privacy van kinderen.

Kinderen worden als extra kwetsbare groep gezien in de wetgeving. Zij zijn zich minder bewust van de gevolgen van hun handelen. Juist ook bij de verwerking van hun persoonsgegevens door sociale media. Daarom krijgen kinderen extra bescherming van de privacywet.

**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** TikTok

**Когда:** 2021.07

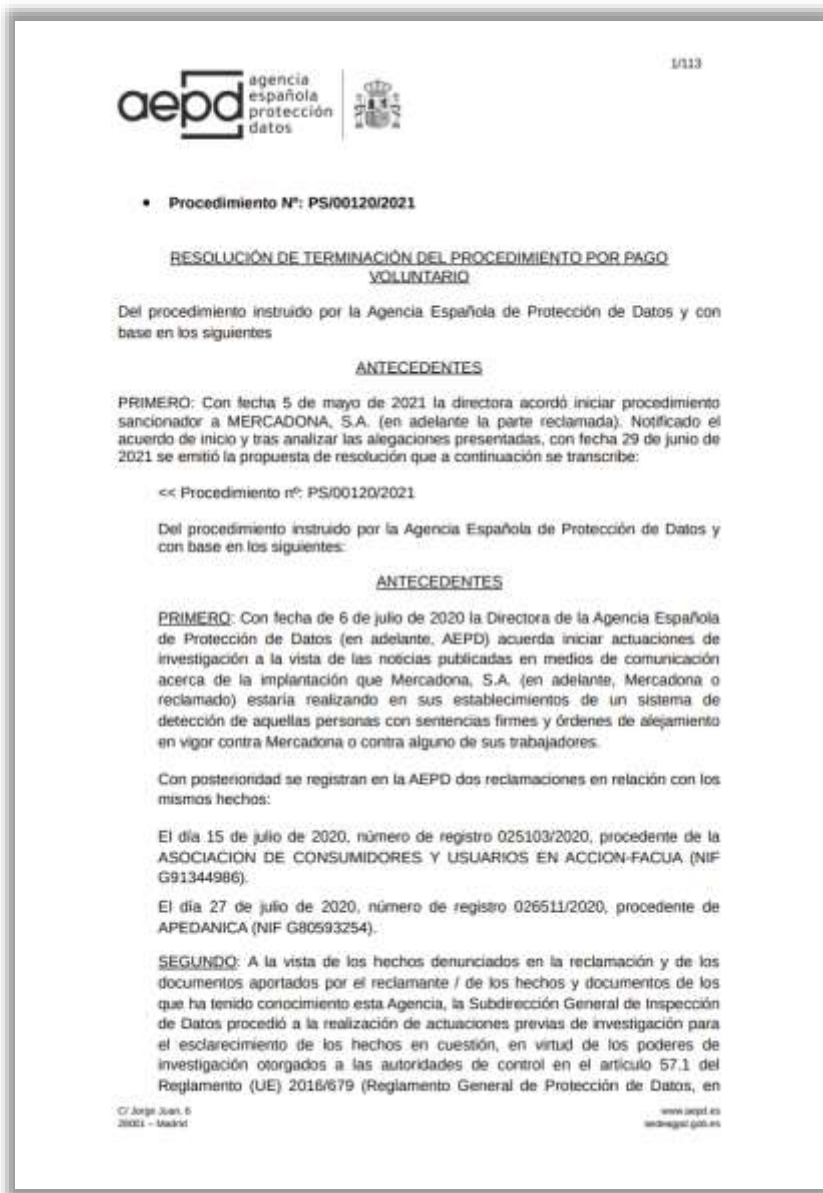
**За что:** нарушение ст. 12 GDPR

**Как:** штраф €750,000

**Причина:** TikTok не опубликовал Privacy Notice на голландском языке, а многие дети, которые используют популярное приложение для обмена видео, не могут понять термины на английском языке. Кроме того, TikTok не смог предоставить адекватного объяснения того, как приложение собирает, обрабатывает и использует персональные данные.

TikTok, у которого около 3,5 миллиона пользователей в Нидерландах, подал апелляцию на штраф. В заявлении платформы говорится, что ее политика приватности доступна на голландском языке с июля 2020 года. На что Регулятор возразил, что штраф касается более раннего периода, когда языковая версия ещё не была доступна пользователям.

## Штраф за незаконное использование системы распознавания лиц посетителей супермаркета



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Mercadona, S.A. (сеть супермаркетов)

**Когда:** 2021.07

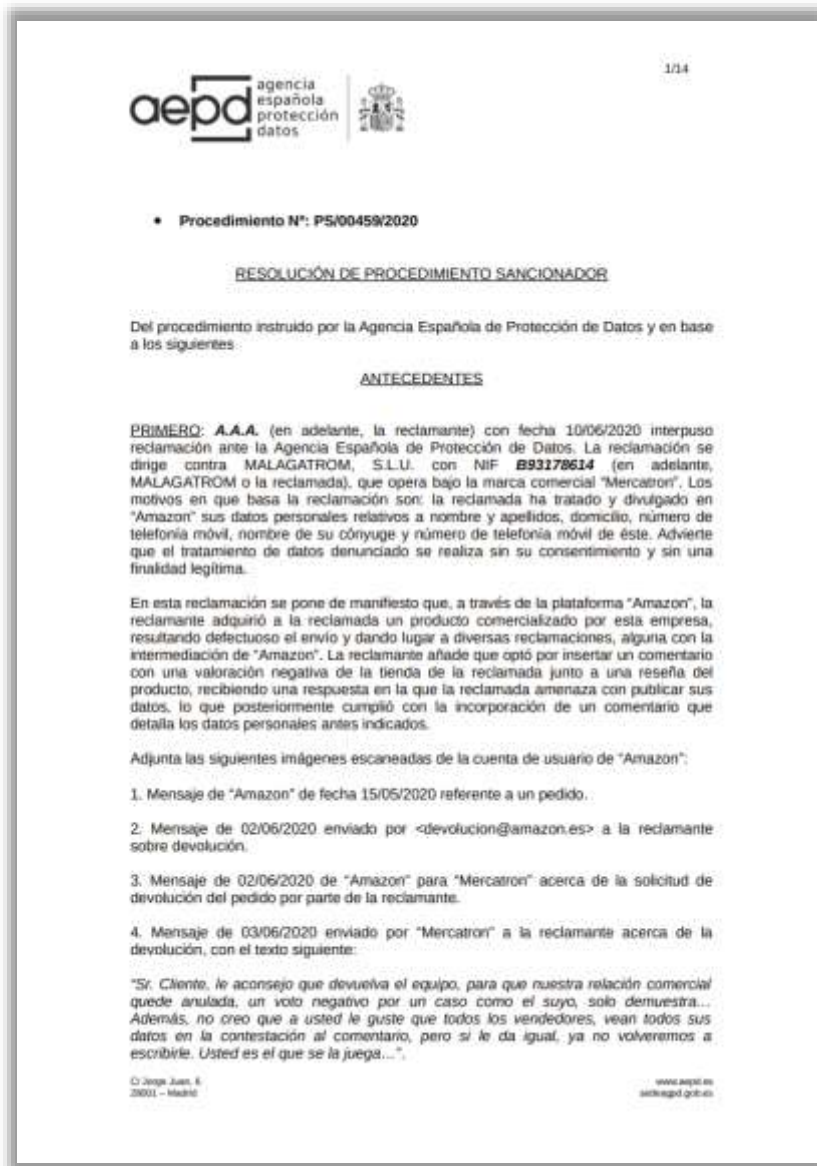
**За что:** нарушение ст. 13, 25 GDPR

**Как:** штраф €2,520,000

**Причина:** в магазинах была установлена система распознавания лиц покупателей, ранее имевших «инциденты» в Mercadona. Система записывала и распознавала лица всех посетителей, включая детей и работников супермаркета. Нарушения:

- отсутствие подходящего правового основания для обработки таких данных;
- нарушение принципов необходимости, пропорциональности и минимизации (контролер выходил за рамки первоначальной цели);
- ошибка при выполнении DPIA) – в нём не учтены специфические риски для работников Mercadona;
- несоблюдение принципов Privacy by design;
- нарушение принципа прозрачности (не было уведомления об обработке).

## Штраф за раскрытие персональных данных покупателя в комментариях



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Malagatrom S.L.U.

**Когда:** 2021.07

**За что:** нарушение ст. 5(1)(f), 6(1) GDPR

**Как:** штрафы €4,000

**Причина:** Заявительница заказала товары из испанского магазина Malagatrom через Amazon и осталась недовольна их качеством из-за имеющихся дефектов. Покупательница предъявила претензии к компании и, как полагается, оставила негативный отзыв в обзоре продукта на странице магазина. В ответ на это продавец не только не предложил мирно решить спор, но и написал текст-предупреждение, в котором призывал всех остерегаться этой покупательницы. Кроме прочего, в комментарии были опубликованы имя, фамилия, адрес, номер телефона заявительницы, а также указывались контактные данные ее мужа.

Представители компании отрицали факт нарушения и утверждали, что комментарии были сделаны во внутреннем чате платформы. Это, конечно, не отвечает действительности, поскольку комментарии на Amazon общедоступны для всех пользователей Интернета даже без регистрации.

## Штраф за множественное нарушение требований GDPR в отношении обработки данных доставщиков



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Deliveroo Italy s.r.l.

**Когда:** 2021.07

**За что:** нарушение ст. 5(1) а), с), е), 13, 22(3), 25, 30(1) с), f), g), 32, 35, 37(7) GDPR

**Как:** штраф €2,500,000

**Причина:** выявлен целый букет нарушений приватности почти 8 тысяч доставщиков:

- использование непрозрачного алгоритма для распределения и управления доставками;
- слежка за доставщиками (геолокация, которая обновляется каждые 12 секунд и хранится 6 месяцев + данные, собираемые во время выполнения заказа, включая всё общение со службой поддержки);
- установленный контролёром период хранения для всех данных в 6 лет;
- не внедрены технические и организационные меры безопасности;
- нет DPIA для обработок данных, касающихся доставщиков.

## Штраф за отказ раскрыть данные несовершеннолетнего пациента его родителю

**Кто:** Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

**Кого:** врач-педиатор

**Когда:** 2021.07

**За что:** нарушение ст. 12(1), 15(1) GDPR

**Как:** штраф €5,000

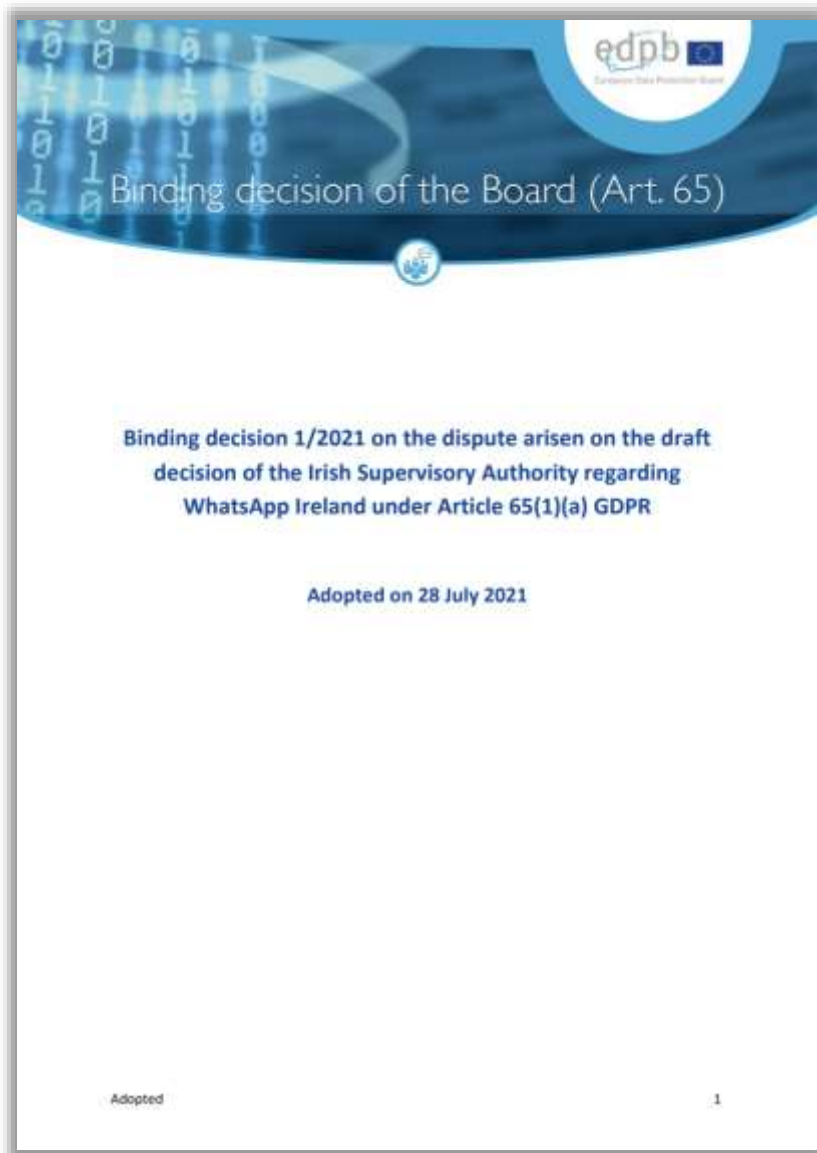
**Причина:** отец несовершеннолетнего, который после развода родителей проживает с матерью, был намерен узнать у педиатра историю болезней и результаты анализов своего ребенка. Заявитель по телефону обратился к врачу и попросил предоставить ему данные медицинской карты ребенка, отправив их по электронной почте.

На свой запрос он получил отказ сразу по нескольким причинам. Во-первых, ответчица указала (врач-педиатор), что больше не является лечащим врачом ребенка и не может предоставить данные о его здоровье. В то же время она не отрицала, что хранит эти данные. Во-вторых, врач отметила, что ранее вела коммуникацию исключительно с матерью ребенка и рассматривает ее как единственного законного представителя. Поскольку педиатр никогда не общалась с Заявителем, она сказала, что единственный способ получить доступ к медицинской карте – приехать Заявителю в клинику лично.

Тот факт, что ответчица больше не является лечащим врачом пациента, не освобождает ее как контролера от обязанности реализовывать права субъекта данных в течение всего срока их хранения. Согласно ст. 14 Кодекса медицинской этики Греции врач должен хранить данные 10 лет с момента последнего обследования.

Поскольку заявитель не лишен родительских прав, он является законным представителем ребенка и может реализовывать право на доступ. Таким образом, отказ педиатра на том основании, что вся информация о здоровье уже была передана матери ребенка, является необоснованным. Заявитель совершает опеку над ребенком и идентифицируется с ним. Более того, требуя личного контакта с Заявителем для предоставления доступа к данным медицинской карты, ответчица создала дополнительные препятствия в доступе, поскольку в условиях пандемии Заявитель не смог приехать в клинику, которая находится в другом городе.

## Рекордный штраф на WhatsApp за нарушение принципа прозрачности



**Кто:** Data Protection Commission (Ирландия)

**Кого:** WhatsApp Ireland Limited

**Когда:** 2021.09

**За что:** нарушение ст. 5(1)(а), 12, 13, 14 GDPR

**Как:** штраф €225,000,000 и предписание устранить нарушения в течение 3 месяцев

**Причина:** WhatsApp (1) не обеспечил предоставление пользователям информации, когда данные предоставляются непосредственно самим субъектом, (2) не обеспечил предоставление необходимой информации субъектам данных, чьи номера телефонов обрабатывались в составе списков контактов пользователей, (3) не обеспечил предоставление информации в простой и доступной форме («easily accessible form»), (4) и, в результате перечисленного, нарушил принцип прозрачности.

Расследование было начато после того, как надзорные органы в разных европейских странах стали получать большое количество жалоб в отношении WhatsApp и его взаимодействия с Facebook. По правилам ст. 56 GDPR данные жалобы должны быть направлены надзорному органу, курирующему основную организационную единицу WhatsApp в ЕС – DPC, который является по отношению к контролеру ведущим надзорным органом (lead supervisory authority) и выполняет функции одного окна (one-shop-stop).

## Штраф за множественное нарушение требований GDPR, в том числе «дикий» телемаркетинг



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Sky Italia S.r.l.

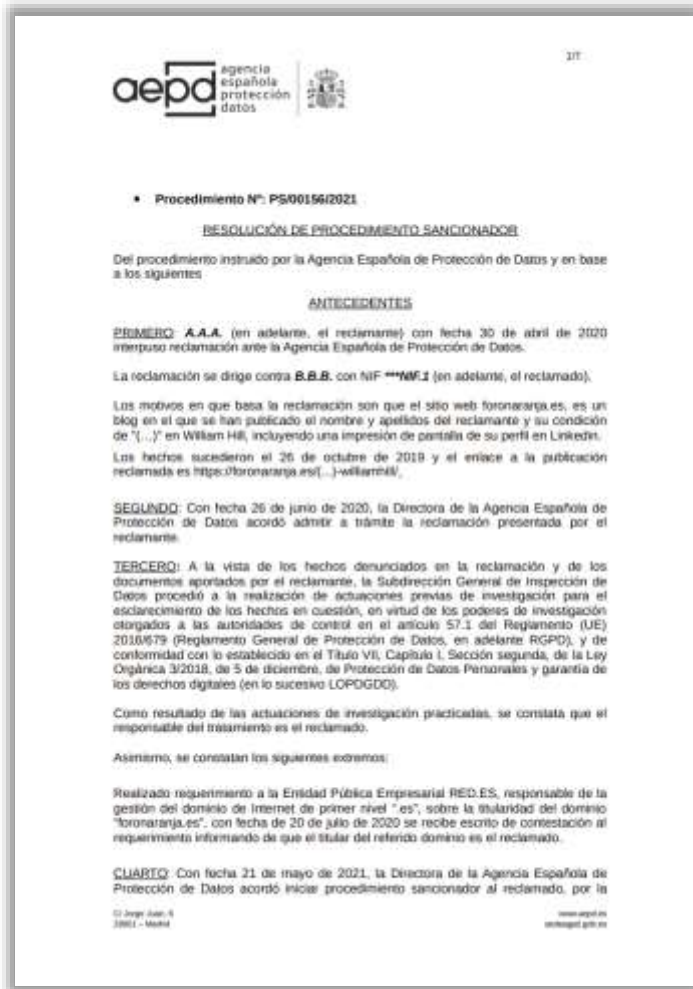
**Когда:** 2021.09

**За что:** нарушение ст. 5(1), 5(2), 6(1), 7, 12(2), 14, 21, 28, 29 GDPR

**Как:** штраф €3,296,326 и запрет обработки данных в рекламных целях с использованием БД, полученных от других компаний

**Причина:** Sky Italia обрабатывала персональные данные, полученные от сторонних компаний, для осуществления телемаркетинговой деятельности, хотя согласие, данное субъектами данных этим компаниям, не предусматривало последующую обработку в целях телемаркетинга.

Кроме того, компания не проводила проверки списков контактов, полученных от вышеупомянутых компаний, и не проверяла их в своем opt-out реестре, в результате чего несколько субъектов данных получили рекламные звонки, несмотря на то, что ранее они возражали против этого.



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** foronaranja.es

**Когда:** 2021.09

**За что:** нарушение ст. 6, 13 GDPR

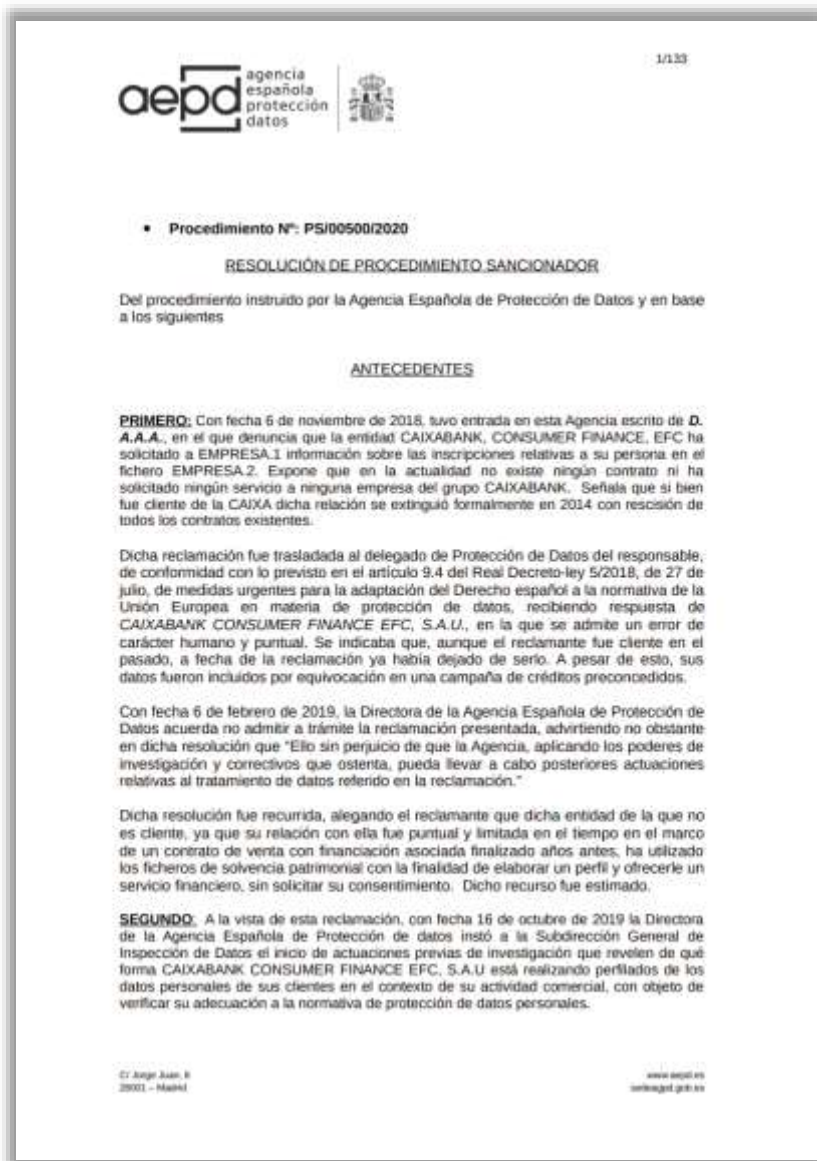
**Как:** штрафы €5,000 и €4,000

**Причина:** некий человек обнаружил скриншот своего LinkedIn профиля на сайте foronaranja.es. Это ему не понравилось и он обратился к надзорному органу (AEPD).

В ходе расследования было установлено, что владелец сайта не получил согласие на обработку данных (это один из тех редких случаев, когда оно действительно было нужно) и не уведомил человека об обработке данных.



## 841 Штраф за нарушения в правовых основаниях обработки данных



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Caixabank Payments & Consumer EFC, EP, S.A.U.

**Когда:** 2021.10

**За что:** нарушение ст.6(1) GDPR

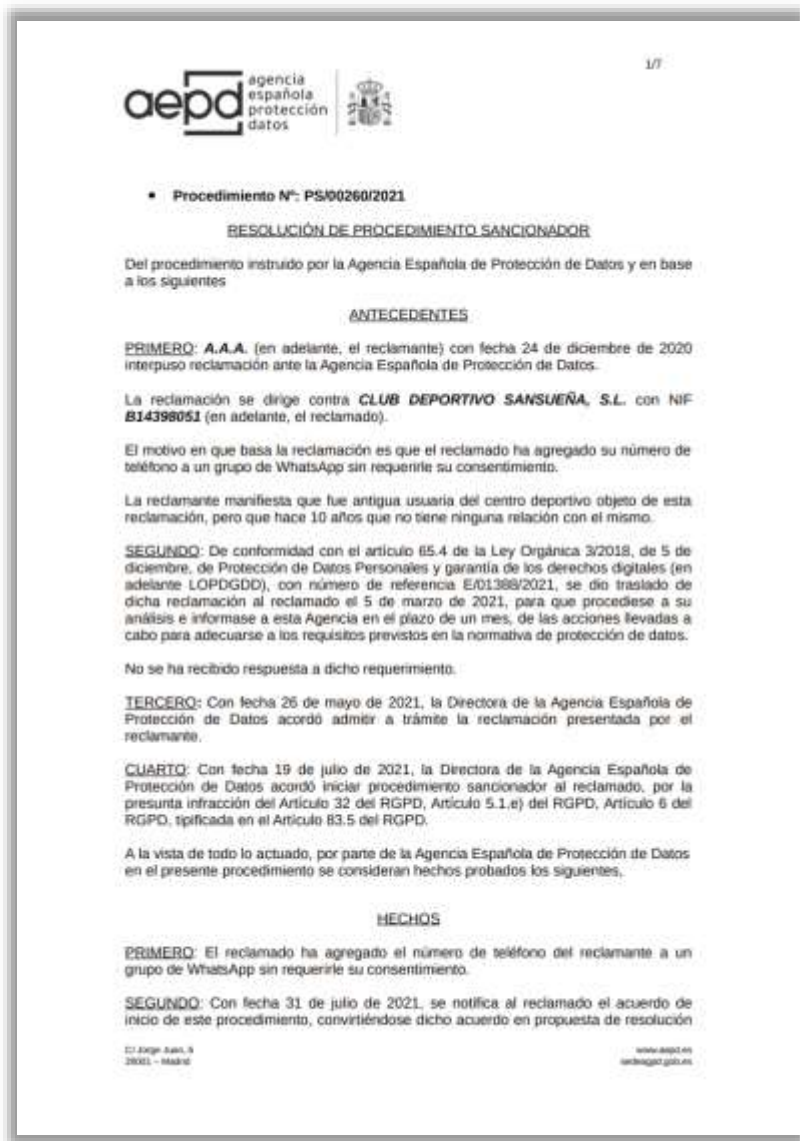
**Как:** штрафы €3,000,000

**Причина:** CaixaBank запросил информацию о субъекте данных (бывавшем клиенте) из бюро кредитных историй, хотя у этого человека не было действующих договоров с банком.

Это лицо также было включено в маркетинговые кампании банка без надлежащего согласия и без предоставления надлежащей информации об обработке данных, включая информации о профилировании, или правовых основаниях, используемых для проведения такой обработки.

Все это произошло даже несмотря на то, что отношения с бывшим клиентом были формально прекращены в 2014 году с расторжением всех действующих контрактов. CaixaBank заявил, что данные субъекта были включены в маркетинговую кампанию по предварительному предоставлению кредитов по ошибке.

## 842 Штраф за добавление в группу в мессенджере без спроса



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Club Deportivo Sansueña, S.L.

**Когда:** 2021.10

**За что:** нарушение ст. 5(1)(e), 6(1), 32(1)(b), 32(1)(d) GDPR

**Как:** штрафы €4,000

**Причина:** Club Deportivo Sansueña добавил субъекта персональных данных в группу в WhatsApp без его предварительного согласия. Человек попал в группу, так как ранее был участником этого клуба, но на момент добавления уже им не являлся.



**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** Bank Millennium S.A.

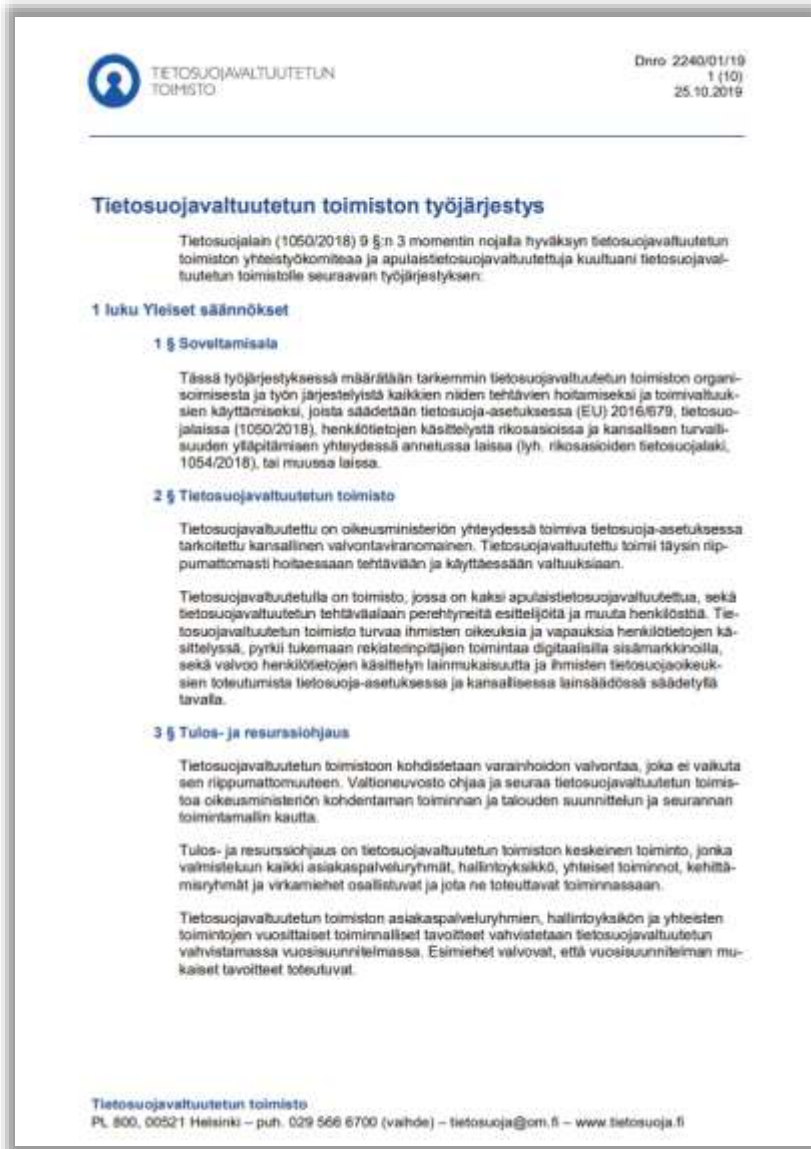
**Когда:** 2021.10

**За что:** нарушение ст. 33(1), 34(1) GDPR

**Как:** штраф €78,000

**Причина:** банк отправлял посылку через службу курьерской доставки. Посылка с ФИО, идентификационными кодами, домашними адресами, номерами аккаунтов и другой информацией была потеряна. Банк решил не сообщать о случившемся ни надзорному органу, ни субъектам персональных данных.

Кто-то об этом узнал и пожаловался в надзорный орган на эту утечку данных. UODO констатировал факт нарушения ст.33 (сообщение об инциденте надзорному органу) и ст.34 (сообщение об инциденте субъектам персональных данных).



**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

**Кого:** Psykoterapiakeskus Vastaamo (центр психотерапии)

**Когда:** 2021.12

**За что:** нарушение ст. 5(1)(f), 32, 33(1), 34(1) GDPR

**Как:** штраф €608,000

**Причина:** в сентябре 2020 года центр психотерапии Vastaamo уведомил надзорный орган Финляндии об атаке на базу данных пациентов центра. Основываясь на техническом расследовании компанией Nixu, занимающейся информационной безопасностью, регулятор приходит к выводу, что Vastaamo должно было знать об утечке еще в марте 2019.

Из-за недостаточности документации Vastaamo также не смог доказать, что соблюдал соответствующие требования безопасности. Таким образом, Vastaamo:

- вовремя не уведомили регуляторный орган и субъектов данных о нарушении защиты персональных данных;
- не защитили собранные данные надлежащим образом;
- не задокументировали меры информационной безопасности.

## Штраф Grindr за передачу данных рекламодателям и недобросовестную модель монетизации

**Кто:** Datatilsynet (Норвегия)

**Кого:** Grindr LLC

**Когда:** 2021.12

**За что:** нарушение ст. 6(1), 9(2) GDPR

**Как:** возможный штраф €6,300,000

**Причина:** приложение для знакомств Grindr, ориентированное на ЛГБТ-сообщество, передавало данные пользователей крупным рекламодателям, в числе которых рекламная платформа MoPub, принадлежащая Twitter. MoPub, в свою очередь, мог делиться этими данными ещё со 100 компаниями-партнёрами.

Одна из причин большого штрафа — особая чувствительность данных (в т.ч. информация о сексуальной ориентации в сочетании с информацией о местоположении пользователей по GPS, IP-адресе, рекламном идентификаторе мобильного телефона, возрасте), которые передавал Grindr. В сочетании с информацией о местоположении сведения о сексуальной ориентации могли бы привести к преследованиям пользователей — например, в Катаре или Пакистане.

Надзорный орган не устроила и модель монетизации Grindr. Одно из преимуществ платной версии приложения — отсутствие таргетированной рекламы, и, как следствие, передачи данных о пользователе рекламодателям. Иначе говоря, пользователь мог гарантировать себе конфиденциальность только при покупке платной версии — что автоматически означает незаконность бесплатной.

В ходе расследования выяснилось, что согласие, полученное компанией Grindr, не было действительным. Пользователи должны были принять политику конфиденциальности, чтобы использовать приложение, но их не спрашивали, согласны ли они на передачу своих данных третьим лицам в маркетинговых целях. Кроме того, информация о раскрытии персональных данных не была достаточно ясной и доступной для пользователей.

## 846 Штраф в €150 млн. ненадлежащий cookie-баннер



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Google LLC и Google Ireland Limited

**Когда:** 2022.01

**За что:** нарушение ст.4(11) GDPR и ст.5(3) ePrivacy Directive

**Как:** штраф €90,000,000 и €60,000,000 + по €100,000 за каждый день задержки в исполнении предписания

**Причина:** cookie-баннер, отображаемый на сайтах google.fr и youtube.com, содержит кнопку, позволяющую немедленно принять файлы cookie, но что пользователю не предлагаются аналогичные средства, позволяющие так же легко отказаться от размещения таких файлов cookie. Иначе говоря, отказаться от сбора cookies можно, если выбрать такую опцию в нескольких разных меню.

Google выдвинула ряд аргументов в свою защиту, в том числе утверждая, что предыдущий штраф CNIL против Google за нарушение файлов cookie от 07.12.2020 все еще находится на рассмотрении Государственного совета, и поэтому это решение должно быть приостановлено, а также утверждается о нарушении принципа *non bis in idem* (т. е. что CNIL не может выносить решения на основе тех же фактов, которые рассматривались в его предыдущих правоприменительных действиях против Google).

CNIL отклонил оба аргумента, подчеркнув, что отложенный характер решения Государственного совета не влияет на компетенцию CNIL накладывать новые санкции, а также указав, что факты текущего дела не идентичны положениям предыдущего решения. CNIL отметил, что предыдущее решение касалось информации пользователей о целях использования файлов cookie, подлежащих согласию, и о средствах отказа от использования файлов cookie, тогда как в данном случае речь идет об условиях самого отказа в согласии, а не связанной с ним информации.

## 847 Штраф в €60 млн. ненадлежащий cookie-баннер

**CNIL.**  
MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL

### Cookies : la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros et FACEBOOK à hauteur de 60 millions d'euros pour non-respect de la loi

06 janvier 2022

*La CNIL a constaté que les sites facebook.com, google.fr et youtube.com ne permettent pas de refuser les cookies aussi simplement que de les accepter. Elle sanctionne GOOGLE à hauteur de 150 millions d'euros et FACEBOOK à 60 millions d'euros et leur enjoint de se mettre en conformité dans un délai de trois mois.*

La formation restreinte, organe de la CNIL chargé de prononcer les sanctions, a constaté, à la suite de contrôles, que les sites web facebook.com, google.fr et youtube.com proposent un bouton permettant d'accepter immédiatement les cookies. En revanche, ils ne mettent pas en place de solution équivalente (bouton ou autre) pour permettre à l'internaute de refuser facilement le dépôt de ces cookies. Plusieurs clics sont nécessaires pour refuser tous les cookies, contre un seul pour les accepter.

La formation restreinte a considéré que ce procédé porte atteinte à la liberté du consentement : dès lors que, sur internet, l'utilisateur s'attend à pouvoir rapidement consulter un site, le fait de ne pas pouvoir refuser les cookies aussi simplement qu'on peut les accepter biaise son choix en faveur du consentement. Cela constitue une violation de l'article 82 de la loi Informatique et Libertés.

Du fait de ce manquement, la formation restreinte de la CNIL a prononcé :

- deux amendes d'un montant total de 150 millions d'euros à l'encontre de GOOGLE (90 millions d'euros pour la société GOOGLE LLC et 60 millions d'euros pour la société GOOGLE IRELAND LIMITED) ;
- une amende de 60 millions d'euros à l'encontre de la société FACEBOOK IRELAND LIMITED.

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Meta Platforms Ireland Limited

**Когда:** 2022.01

**За что:** нарушение ст.4(11) GDPR

**Как:** штраф €60,000,000 + по €100,000 за каждый день задержки в исполнении предписания

**Причина:** facebook.com не предоставил пользователям средства для свободного предоставления их согласия, поскольку баннер файлов cookie на facebook.com не позволяет пользователям отказываться от файлов cookie с той же степенью простоты, как их принять. Иначе говоря, пользователю нужно сначала согласиться со сбором cookies, а потом уже найти опцию отказаться от них.



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Enel Energia S.p.A

**Когда:** 2022.01

**За что:** нарушение ст. 5(1)(a), 5(1)(d), 5(2), 6(1), 12, 13, 21, 24, 25(1), 30, 31 GDPR

**Как:** штраф €26,513,977

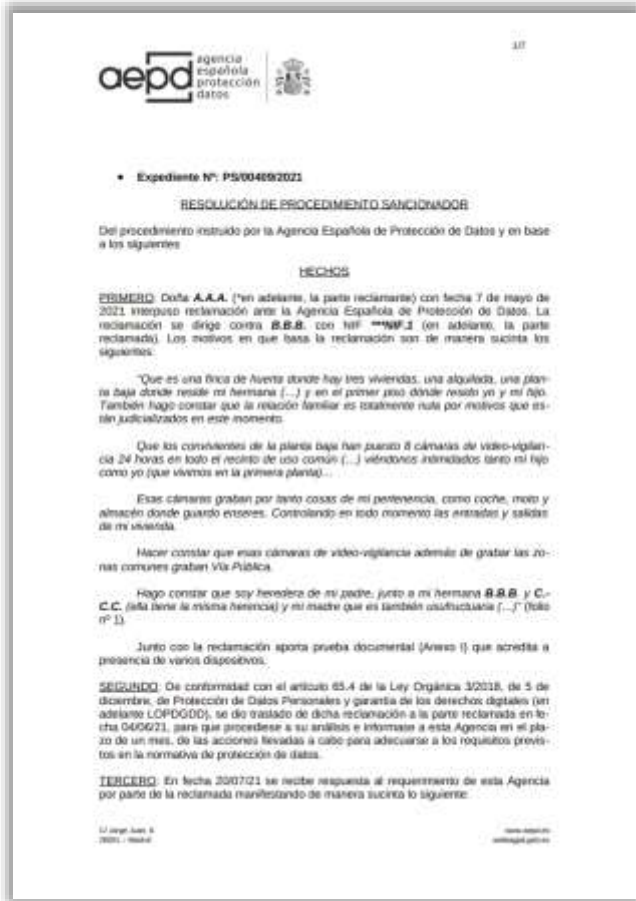
**Причина:** многочисленные жалобы на получение нежелательных рекламных звонков, в том числе предварительно записанных, а также различные проблемы, связанные с обработкой персональных данных в контексте услуг по энергоснабжению, включая действия по обработке, осуществляемые через специальный раздел веб-сайта Enel Energia и соответствующее приложение.

Утверждения компании о том, что номера, использованные для телефонных звонков в рекламных целях, не принадлежали ни самой компании, ни ее деловым партнерам, являются подтверждением отсутствия у Enel Energia эффективных средств противодействия незаконным рекламным звонкам, проводимым от имени компании, особенно с учетом того, что компания напрямую получала жалобы на агрессивную практику телемаркетинга.

Записи о субъектах в базах компании были неупорядочены, что привело к незаконной передаче данных, субъект одним согласием «авторизовал» различные виды обработки, а на веб-сайте Enel Energia было две записи о контролере данных, и одна противоречила другой.



## 849 Штраф за публикацию BDSM-фотографий



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** частное лицо

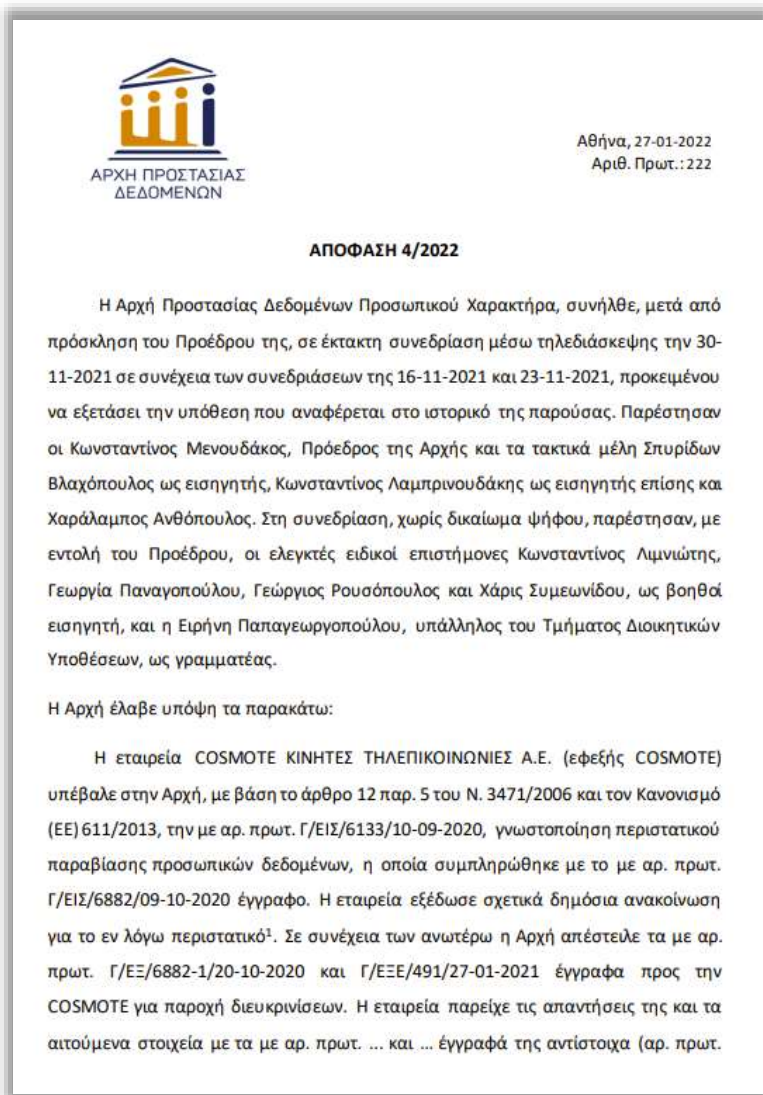
**Когда:** 2022.01

**За что:** нарушение ст. 5(1)(c) GDPR

**Как:** штрафы €1,500

**Причина:** в 2020 года фотографии из сексуальной жизни заявителя были опубликованы на личном веб-сайте его/её супруга/и (пол сторон по делу не указывается). На фотографиях лицо заявителя было размыто большими пикселями. Имя заявителя также не указывалось, однако сам сайт был приурочен к разводу, что могло дать наводку на личность человека на фото. В 2013 году супруги подписали так называемый BDSM-submission contract. Контракт содержал пункт, в котором субъект данных отказывался от права на приватность, соглашаясь стать «рабом», и позволял ответчику демонстрировать все, что связано с субъектом данных. Договор позволял каждой из сторон расторгнуть его в любой момент.

Согласие на участие в каком-либо мероприятии, либо же наличие контракта между сторонами не обязательно равно согласию на обработку персональных данных (публикацию фотографий). Для согласия как правового основания ставятся специальные требования ст.7 GDPR, детализированные в руководстве WP29 о согласии. Более того, регулятор ещё раз напомнил, что любой отказ от основоположных прав, закреплённых в Конституции или Европейской Хартии прав, не имеет юридической силы. Ответчику также было отказано в аргументах, что сайт использовался для личных целей или что фотографии с заявителем были "анонимизированы".



**Κτο:** Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

**Κοго:** Cosmote Mobile Telecommunications S.A.

**Когда:** 2022.01

**За что:** нарушение ст. 5(1)(а), 5(2), 13, 14, 25(1), 26, 28, и 35(7) GDPR

**Как:** штраф €6,000,000

**Причина:** Cosmote сообщил об утечке данных в надзорный орган о скомпрометированном результате действий хакеров файле, содержащем данные об абонентском трафике, которые, с одной стороны, хранятся в течение 90 дней с момента совершения звонков для целей управления проблемами и потенциальными сбоями, а с другой С другой стороны, файл анонимизируется и хранится в течение 12 месяцев, чтобы сделать статистические выводы в отношении оптимального дизайна сети мобильной телефонной связи после добавления дополнительных персональных данных. В результате расследования было обнаружено, что в ходе этой же атаки был взломан веб-сайт, размещенный в инфраструктуре OTE Group. В частности, хакеру удалось получить административный доступ, используя пароль администратора OTE Group, а затем выполнить запросы в системе Data Lake Cosmote.

## Штраф за несоблюдения требований к безопасности обработки данных



Αθήνα, 27-01-2022  
Αριθ. Πρωτ.: 222

### ΑΠΟΦΑΣΗ 4/2022

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε, μετά από πρόσκληση του Προέδρου της, σε έκτακτη συνεδρίαση μέσω τηλεδιάσκεψης την 30-11-2021 σε συνέχεια των συνεδριάσεων της 16-11-2021 και 23-11-2021, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Κωνσταντίνος Μενουδάκος, Πρόεδρος της Αρχής και τα τακτικά μέλη Σπυρίδων Βλαχόπουλος ως εισηγητής, Κωνσταντίνος Λαμπρινουδάκης ως εισηγητής επίσης και Χαράλαμπος Ανθόπουλος. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν, με εντολή του Προέδρου, οι ελεγκτές ειδικοί επιστήμονες Κωνσταντίνος Λιμνιώτης, Γεωργία Παναγοπούλου, Γεώργιος Ρουσόπουλος και Χάρης Συμεωνίδου, ως βοηθά εισηγητή, και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Η εταιρεία COSMOTE ΚΙΝΗΤΕΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ Α.Ε. (εφεξής COSMOTE) υπέβαλε στην Αρχή, με βάση το άρθρο 12 παρ. 5 του Ν. 3471/2006 και τον Κανονισμό (ΕΕ) 611/2013, την με αρ. πρωτ. Γ/ΕΙΣ/6133/10-09-2020, γνωστοποίηση περιστατικού παραβίασης προσωπικών δεδομένων, η οποία συμπληρώθηκε με το με αρ. πρωτ. Γ/ΕΙΣ/6882/09-10-2020 έγγραφο. Η εταιρεία εξέδωσε σχετικά δημόσια ανακοίνωση για το εν λόγω περιστατικό<sup>1</sup>. Σε συνέχεια των ανωτέρω η Αρχή απέστειλε τα με αρ. πρωτ. Γ/ΕΞ/6882-1/20-10-2020 και Γ/ΕΞΕ/491/27-01-2021 έγγραφα προς την COSMOTE για παροχή διευκρινίσεων. Η εταιρεία παρείχε τις απαντήσεις της και τα αιτούμενα στοιχεία με τα με αρ. πρωτ. ... και ... έγγραφα της αντίστοιχα (αρ. πρωτ.

**Κτο:** Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

**Κογο:** Hellenic Tele Communications Organization SA, OTE Group

**Κοгда:** 2022.01

**За что:** нарушение ст. 32(1) GDPR

**Как:** штраф €3,250,000

**Причина:** Cosmote Mobile Telecommunication SA сообщил об утечке данных в надзорный орган и представил различные документы, из которых следует, что OTE Group должна была участвовать в расследовании инцидента, особенно в отношении принятых мер безопасности, но это не было сделано. Надзорный орган считает, что и Cosmote, и OTE Group несут ответственность за определение и реализацию технических и организационных мер безопасности данных.

## Штраф на IAB Europe за множественные нарушения GDPR в контексте Transparency and Consent Framework

**Кто:** l'Autorité de protection des données (Бельгия)

**Кого:** Advertising Bureau Europe ('IAB Europe')

**Когда:** 2022.02

**За что:** нарушение ст. 5(1)(a), 5(1)(f), 6, 12, 14, 24, 25, 30, 32, 25, 37, 38 и 39 GDPR

**Как:** штраф €250,000, 6 месяца на выполнение [согласованного плана по исправлению нарушений](#) и предписание уничтожить данные

**Причина:** DPA постановил, что все данные, собранные посредством принятого в Европе механизма Transparency & Consent Framework (TCF), были получены незаконно и подлежат уничтожению. Решение затронет интересы более тысячи специализирующихся на онлайн-рекламе компаний, которые состоят в ассоциации IAB Europe, в том числе Google, Amazon и Microsoft.

Большей частью рекламы в Европе управляет отраслевая ассоциация IAB Europe — она была создана с тем, чтобы рекламодатели и рекламные площадки действовали единообразно и подчинялись требованиям местного законодательства. Для этого был разработан единый механизм Transparency and Consent Framework (TCF): при заходе на сайты пользователи видели всплывающие окна, запрашивающие их согласие на обработку данных.

Данные каждого пользователя собирались на различных ресурсах и включали довольно подробную информацию, которая представлялась в формате TC String. Эти данные, по сути, транслировались онлайн неограниченному кругу лиц без какого-либо надзора и обрабатывались системой RTB (Real-Time Bidding) — аукционом с автоматическими ставками в реальном времени, определяющим, какая реклама демонстрируется пользователям на площадке.

IAB Europe считает, что предпочтения пользователей в коде TC String не являются персональными данными. Регулятор с этим не согласился и заявил, что с помощью этих данных можно идентифицировать конкретное физическое лицо (п. 309-310 решения).

Также IAB Europe не рассматривала себя контролёром и всю ответственность оставляла на рекламодателях и платформах. Регулятор же определил, что все участники TCF и сама ассоциация являются совместными контролёрами (п. 370, 402 решения), поскольку они все пользователи общей экосистемы TCF и каждый имеет ту или иную роль, которая реализуется в общей цели функционирования TCF.

Также см. [решение](#) Суда Европейского Союза (CJEU) от 07.03.2024 по делу C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit*.

<https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr>

<https://iabeuropa.eu/all-news/apd-ruling-clears-way-for-work-on-developing-tcf-into-a-formal-gdpr-code-of-conduct-iab-europe-statement-on-the-apd-decision-announced-today/>

## Штраф за неприменение мер безопасности, предотвращающих мошенническое копирование SIM-карт

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Vodafone España, S.A.U.

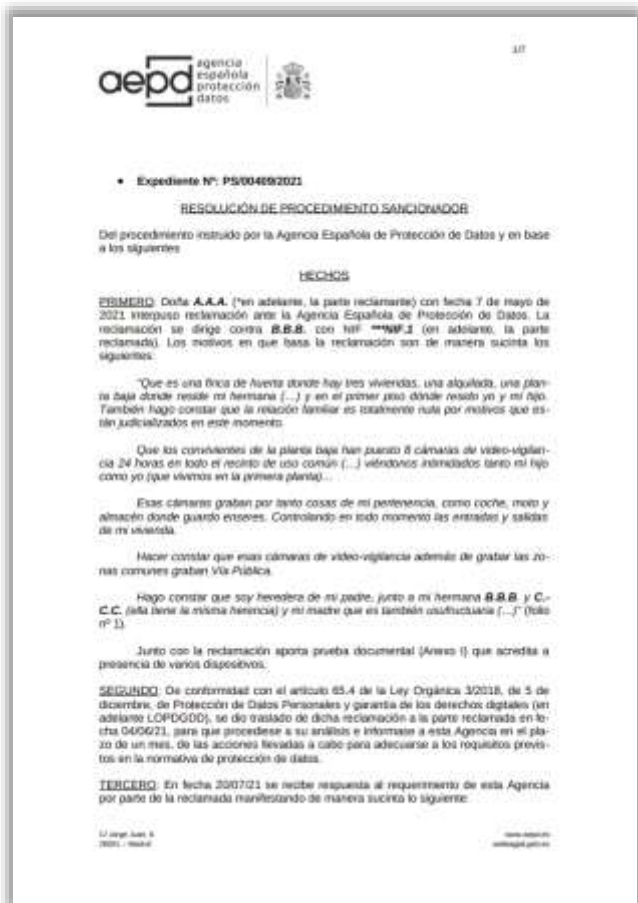
**Когда:** 2022.02

**За что:** нарушение ст. 5(1)(f) и 5(2) GDPR

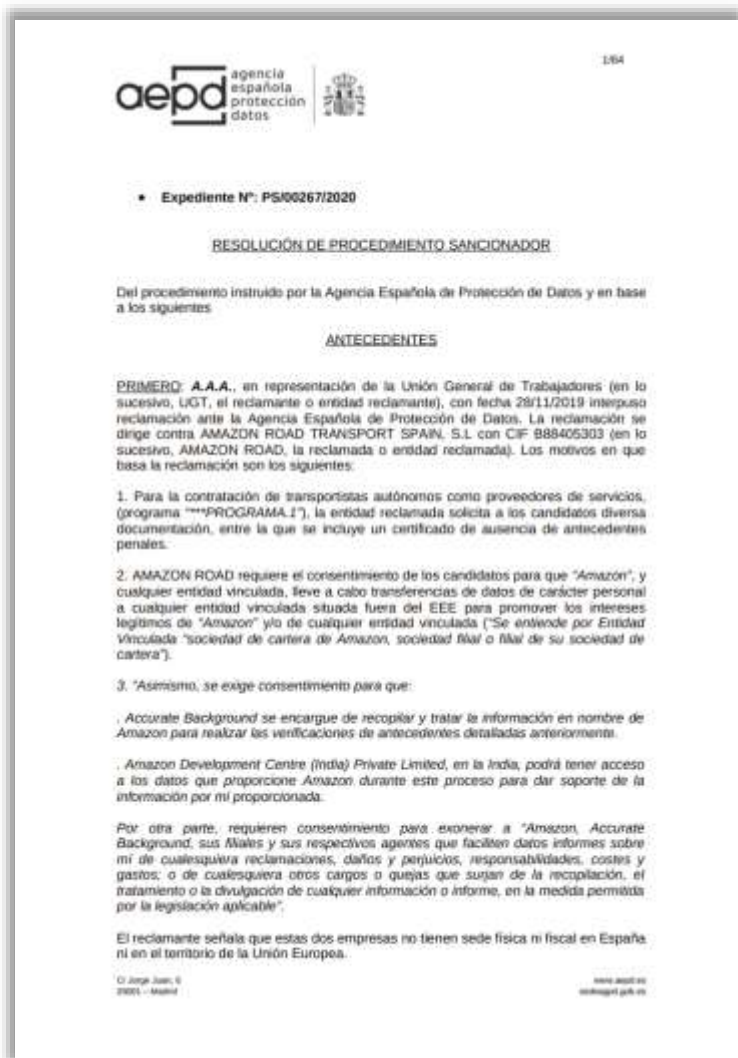
**Как:** штраф €3,940,000

**Причина:** девять клиентов подали в AEPD жалобы на Vodafone после того, как стали жертвами мошенничества из-за противоправного использования их SIM-карт путем осуществления различных банковских переводов через онлайн-банкинг и покупок за счет пострадавших.

Vodafone должным образом не верифицировал личность лиц (мошенников), обратившихся за выпуском дубликатов SIM-карт. Кроме того, Vodafone не смог доказать эффективность мер, принятых для предотвращения кражи персональных данных.



## 854 Штраф за незаконную обработку данных о судимости



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Amazon Road Transport Spain S.L.

**Когда:** 2022.02

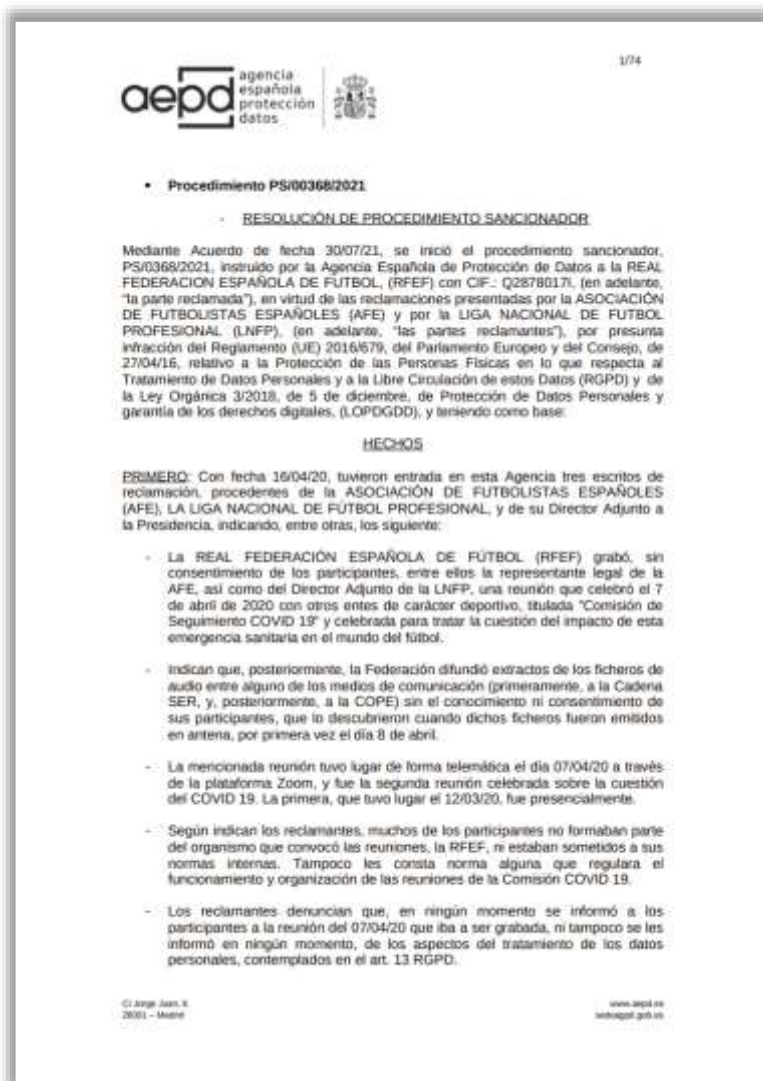
**За что:** нарушение ст. 6(1) и 10 GDPR

**Как:** штраф €2,000,000

**Причина:** жалоба представителя Испанского профсоюза работников, согласно которой при найме самозанятых подрядчиков Amazon Road Transport запросил справки об отсутствии судимости, т.е. отрицательные справки, специально требуя согласия кандидатов, чтобы эти данные могли быть переданы компаниям группы и их поставщикам, расположенным за пределами Европейской экономической зоны.

AEPD согласился с доводами жалобы об отсутствии у Amazon надлежащей процедуры для сбора и последующей обработки персональных данных о судимости, но отклонил доводы о нарушении Amazon ст. 7 и 49(1) GDPR, касающихся международной передачи данных.

## 855 Штраф за незаконную обработку видеозаписи встречи в Zoom



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Real Federación Española de Fútbol

**Когда:** 2022.02

**За что:** нарушение ст. 6(1) и 13(3) GDPR

**Как:** штраф €200,000

**Причина:** распространение видеозаписи встречи, проведенной в Zoom, без ведома или согласия участников, представляющих другие организации, а также за непредоставление участникам встречи Privacy Notice. Согласно выводам регулятора, иконки видеозаписи встречи в Zoom недостаточно для информирования участников – о записи встречи необходимо сообщить напрямую. Также было указано, что дальнейшее распространение видеозаписи было осуществлено без законного основания (контролер ссылался на свой законный интерес), т.к. можно было ограничиться публикацией текстовой расшифровки (протокола) встречи.



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Clearview AI, Inc.

**Когда:** 2022.02

**За что:** нарушение ст. 5(1)(a), 5(1)(b), 5(1)(e), 6, 9, 12, 13, 14, 15, 27 GDPR

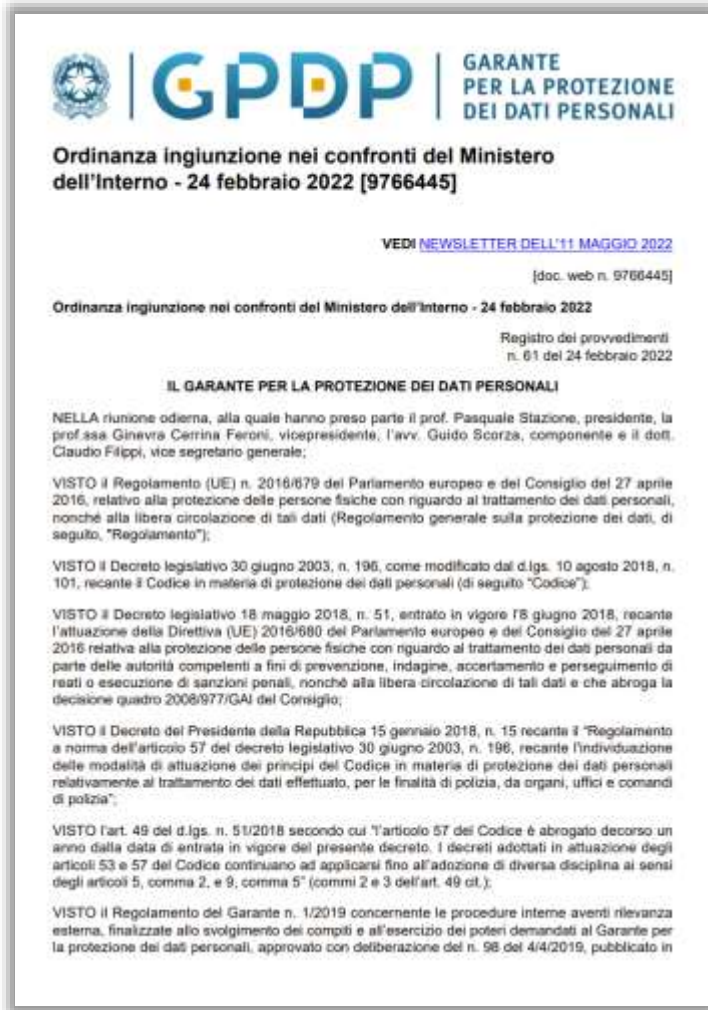
**Как:** штраф €20,000,000 и несколько предписаний – удалить данные субъектов из Италии; прекратить сбор и дальнейшую обработку персональных данных в системе распознавания лиц; назначить в течение 30 дней представителя в ЕС.

**Причина:** Clearview AI находится в США и владеет базой данных из 10 миллиардов изображений лиц людей со всего мира, которые извлекаются из общедоступных веб-источников, а также с применением технологий ИИ формирует профили людей с помощью извлеченной из изображений биометрии и связанных с изображениями метаданных.

Персональные данные, включая биометрические данные и информацию о геолокации, были обработаны компанией без надлежащего правового основания, поскольку законный интерес американской компании не может квалифицироваться таким образом. Кроме того, компания нарушила несколько основных принципов GDPR, таких как прозрачность, ограничение цели и ограничение срока хранения; компания не предоставила субъектам данных информацию, указанную в ст.13-14 GDPR, не предоставила по запросам субъектов информацию об обработке персональных данных в соответствии со ст.15 GDPR в установленные сроки, а также не назначила представителя в ЕС.



## Штраф за незаконное распространение видео и изображений арестованных лиц



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** МВД Италии

**Когда:** 2022.02

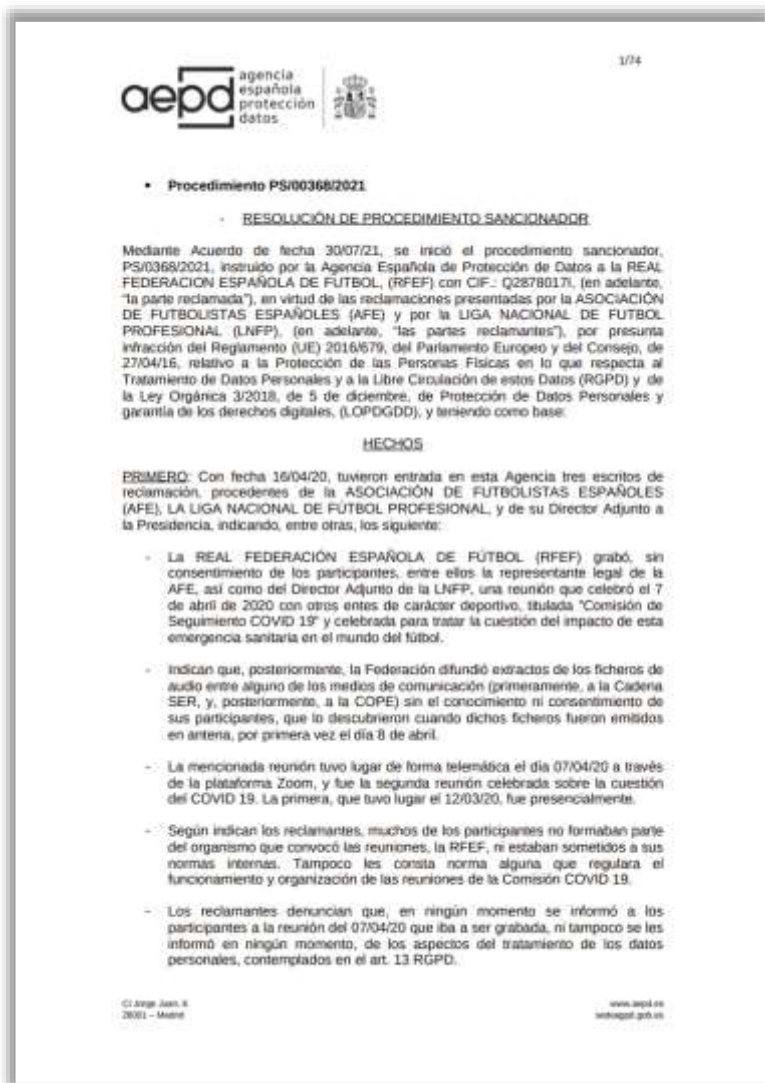
**За что:** нарушение ст. 3(1)(a), 3(1)(c), 5(1)(a) Law Enforcement Directive

**Как:** штраф €60,000

**Причина:** надзорный орган получил информацию о публикации на различных веб-сайтах и в газетах видео и изображений с логотипом Государственной полиции, демонстрирующих операции по задержанию, проведенные неназванным полицейским участком в отношении восьми подозреваемых (включая заявителя жалобы), предположительно ответственных за ряд уголовных правонарушений. Также было обнаружено, что рассматриваемое видео содержало крупные планы арестованных лиц с указанием их имен под каждым изображением, а само видео было доступно на Facebook и YouTube в течение 5 лет.

DPA решил, что публикация видео и фотоснимков разрешена только в целях правосудия или по соображениям общественного интереса. Однако в рассматриваемом случае не было необходимости раскрывать изображения или дополнительные подробности, предоставленные прессе. Таким образом, полицейский участок осуществил ненужную, чрезмерную и вредную обработку данных, которая задевает достоинство вовлеченных субъектов данных.

## 858 Штраф за незаконную обработку видеозаписи встречи в Zoom



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Baser Comercializadora De Referencia, SA

**Когда:** 2022.02

**За что:** нарушение ст. 6(1) и 13(3) GDPR

**Как:** штраф €200,000

**Причина:** распространение видеозаписи встречи, проведенной в Zoom, без ведома или согласия участников, представляющих другие организации, а также за непредоставление участникам встречи Privacy Notice. Согласно выводам регулятора, иконки видеозаписи встречи в Zoom недостаточно для информирования участников – о записи встречи необходимо сообщить напрямую. Также было указано, что дальнейшее распространение видеозаписи было осуществлено без законного основания (контролер ссылался на свой законный интерес), т.к. можно было ограничиться публикацией текстовой расшифровки (протокола) встречи.

## 859 Штраф на Meta за нарушение безопасности обработки данных



**Кто:** Data Protection Commission (Ирландия)

**Кого:** Meta Platforms Ireland Limited

**Когда:** 2022.03

**За что:** нарушение ст. 5(1)(f), 5(2), 24(1), 32(1) GDPR

**Как:** штраф €17,000,000 и предписание устранить нарушения в течение 3 месяцев

**Причина:** серия из 12 эпизодов нарушения безопасности обработки данных, уведомления о которых были получены DPC за шестимесячный период с 7 июня 2018 г. по 4 декабря 2018 г. В результате своего расследования DPC обнаружил, что Meta Platforms нарушают статьи 5 (2) и 24 (1) GDPR. DPC обнаружил, что у Meta Platforms не было соответствующих технических и организационных мер, которые позволили бы компании продемонстрировать обеспечение мер безопасности в отношении данных пользователей из ЕС.

## 860 Штраф за нарушение принципа «подотчётности» (accountability)



### Danske Bank indstilles til bøde

Dato: 05-04-2022

Nyhed

Datatilsynet vurderer, at Danske Bank ikke har kunnet dokumentere, at de har slettet personlysninger i overensstemmelse med databeskyttelsesreglerne, og tilsynet har derfor indstillet banken til en bøde på 10 mio. kr.



Datatilsynet har anmeldt Danske Bank til politiet og indstillet banken til bøde på 10 mio. kr. Det sker i forlængelse af, at tilsynet i november 2020 indledte en sag af egen drift, efter at banken selv havde oplyst, at de havde identificeret et problem med sletning af personoplysninger, som der ikke nødvendigvis var en forretningsmæssig begrundelse for fortsat at behandle.

**Кто:** Datatilsynet (Дания)

**Кого:** Danske Bank

**Когда:** 2022.04

**За что:** нарушение ст. 5(2) GDPR

**Как:** штраф €1,300,000, дело передано в полицию

**Причина:** в ходе расследования выяснилось, что банк в более чем 400 своих системах не смог продемонстрировать, были ли документально установлены сроки хранения и автоматического уничтожения персональных данных, а также было ли уничтожение персональных данных выполнено вручную. Эти системы обрабатывают персональные данные миллионов клиентов банка.

## Министр финансов Нидерландов оштрафован за нарушение принципов GDPR



**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** министр финансов Нидерландов

**Когда:** 2022.04

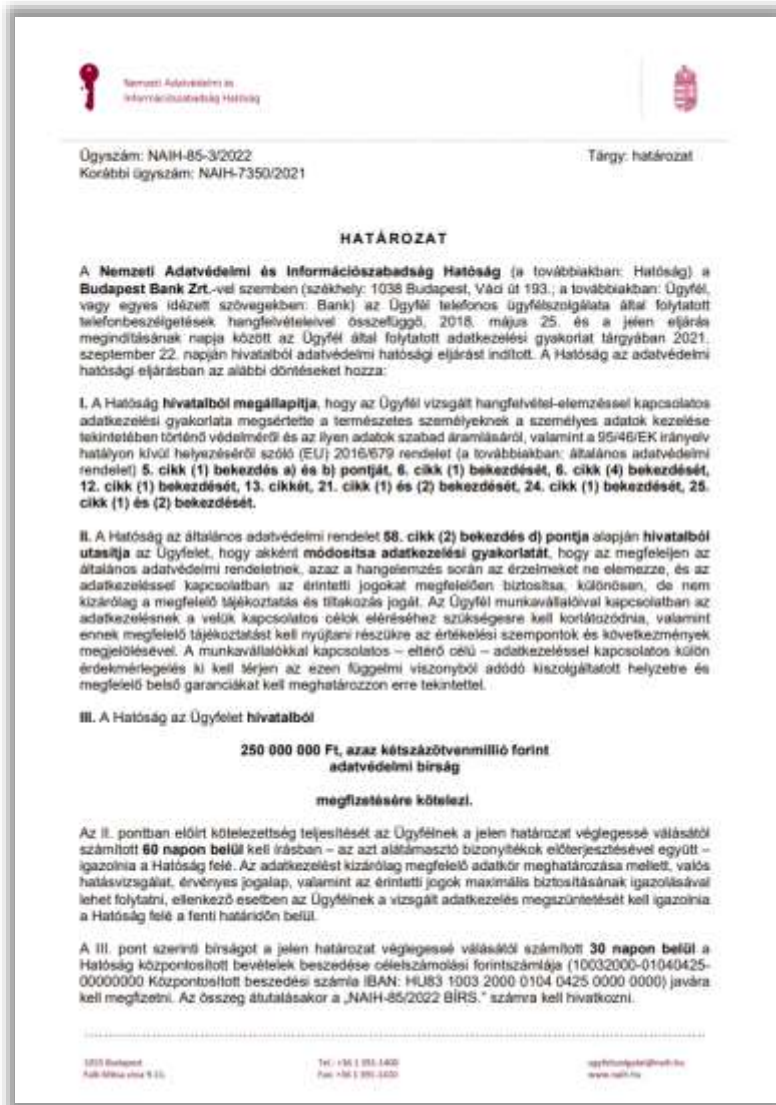
**За что:** нарушение ст. 5(1)(a), 5(1)(b), 5(1)(d), 5(1)(e), 6(1), 32(1) и 35(2) GDPR

**Как:** штраф €3,700,000

**Причина:** в 2021г. было проведено расследование в отношении обработки персональных данных в мобильном приложении «FSV», предназначенном для оповещения органов власти Нидерландов о возможных фактах мошенничества. За период с 2013 по 2020 годы в FSV была обработана информация о 244,000 физических лиц (включая несовершеннолетних) и 30,000 предпринимателей. Хотя непосредственно обработку данных, включающих в себя сведения о здоровье, гражданстве и уголовной ответственности, осуществляла Налогово-таможенная администрация Нидерландов, но в качестве контролёра данных был квалифицирован министр финансов.

Надзорный орган подчеркнул, что налоговые органы действовали с нарушением принципов законности, целевого назначения, точности и ограничения периода хранения персональных данных в FSV.

## Штраф за неправомерное использование технологий искусственного интеллекта при анализе звонков клиентов



**Кто:** Nemzeti Adatvédelmi és Információszabadság Hatóság (Венгрия)

**Кого:** Budapest Bank Zrt.

**Когда:** 2022.02

**За что:** нарушение ст. 5, 6, 12, 13, 21, 24, 25 GDPR

**Как:** штраф €653,000 и предписание изменить процесс обработки персональных данных в срок 60 дней

**Причина:** банк с использованием технологий искусственного интеллекта (ИИ) осуществлял анализ записей телефонных переговоров с клиентами. По результатам анализа эмоционального состояния клиента и используемых им ключевых слов ИИ в автоматическом режиме формировал рейтинг клиентов, в отношении которых рекомендовалось выполнить повторный (обратный) звонок. По мнению банка, законным основанием для такой обработки является законный интерес самого банка.

Надзорный орган указал, что единственным правовым основанием для анализа голоса и эмоционального состояния человека может быть только свободно предоставленное и информированное согласие субъекта данных. Кроме того, проеденное банком DPIA не предусматривало принятие адекватных мер по снижению рисков для субъектов данных.

## Штраф на процессора за утечку данных и ненадлежащий Data Processing Agreement



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Dedalus Biologie

**Когда:** 2022.04

**За что:** нарушение ст.28(3), 29, 32 GDPR

**Как:** штраф €1,500,000

**Причина:** 23.02.2021г. СМИ опубликовали сведения об утечке персональных данных почти 500,000 человек из двух лабораторий, обслуживаемых Dedalus Biologie – поставщиком SaaS-решения для осуществления медицинских анализов. Скомпрометированные данные включали медицинскую информацию (например, болезни, генетические заболевания, беременность, медикаментозное лечение, генетические данные).

SaaS-провайдер (как процессор данных) был признан виновным не только в принятии недостаточных технических и организационных мер по защите утекших данных, но и в нарушении требований к содержанию Data Processing Agreement, заключаемого с потребителями SaaS-решения.

## Штраф за отсутствие эффективной процедуры идентификации клиентов

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Baser Comercializadora De Referencia, SA

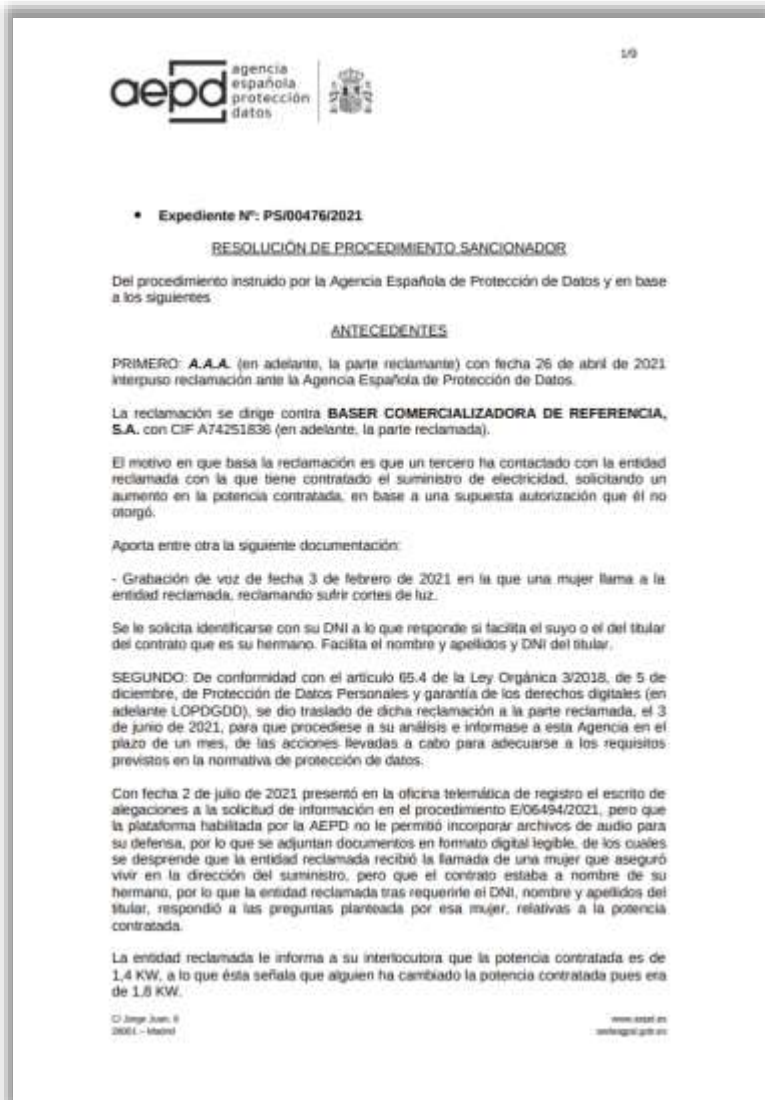
**Когда:** 2022.04

**За что:** нарушение ст. 6 и 32 GDPR

**Как:** штрафы €100,000 (ст.6) и €50,000 (ст.32)

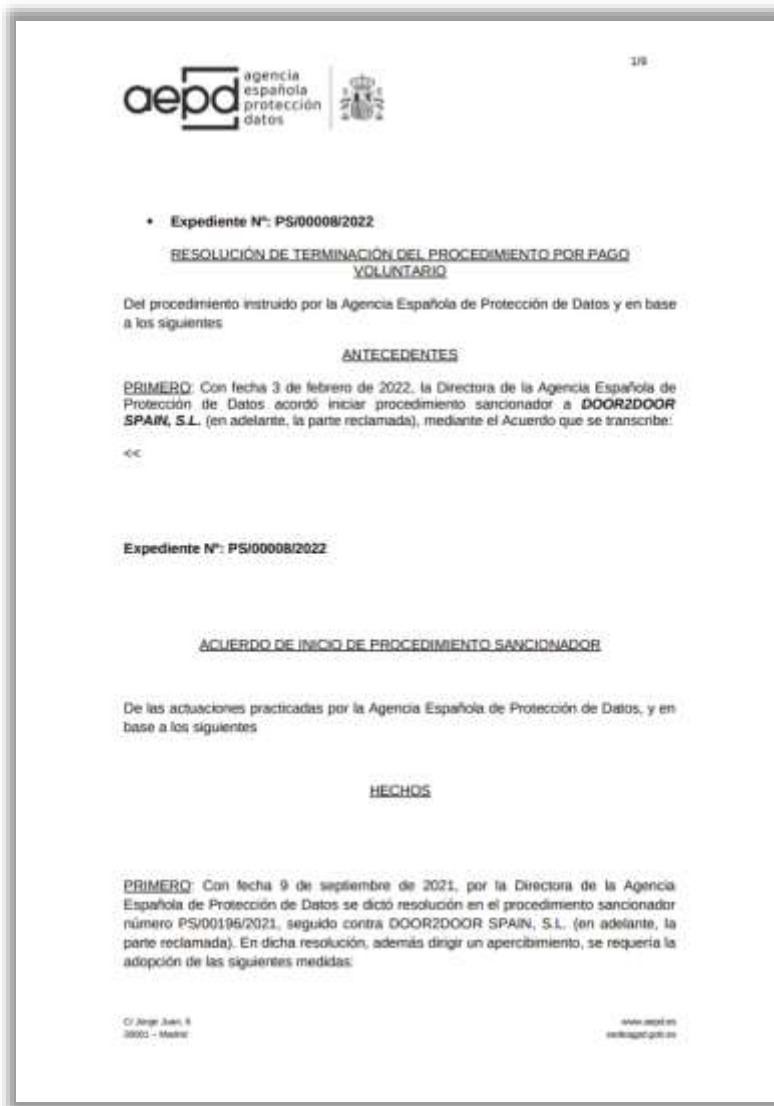
**Причина:** жалоба клиента компании, который утверждал, что контракт с компанией был изменен без его согласия. Компания утверждала, что ранее с ней связалось некое лицо, указавшее данные клиента и запросившее изменения условия контракта.

АEPD указал, что Baser Comercializadora не смогла продемонстрировать наличие эффективной процедуры идентификации клиентов, а запрос у обращающихся лиц таких данных как имена, фамилии, номера телефонов и адреса не является надлежащей практикой, т.к. эти данные могут быть доступны третьим лицам и использоваться в мошеннических целях.





## 865 Штраф за невыполнение ранее полученного предписания



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** DOOR2DOORSPAIN SL

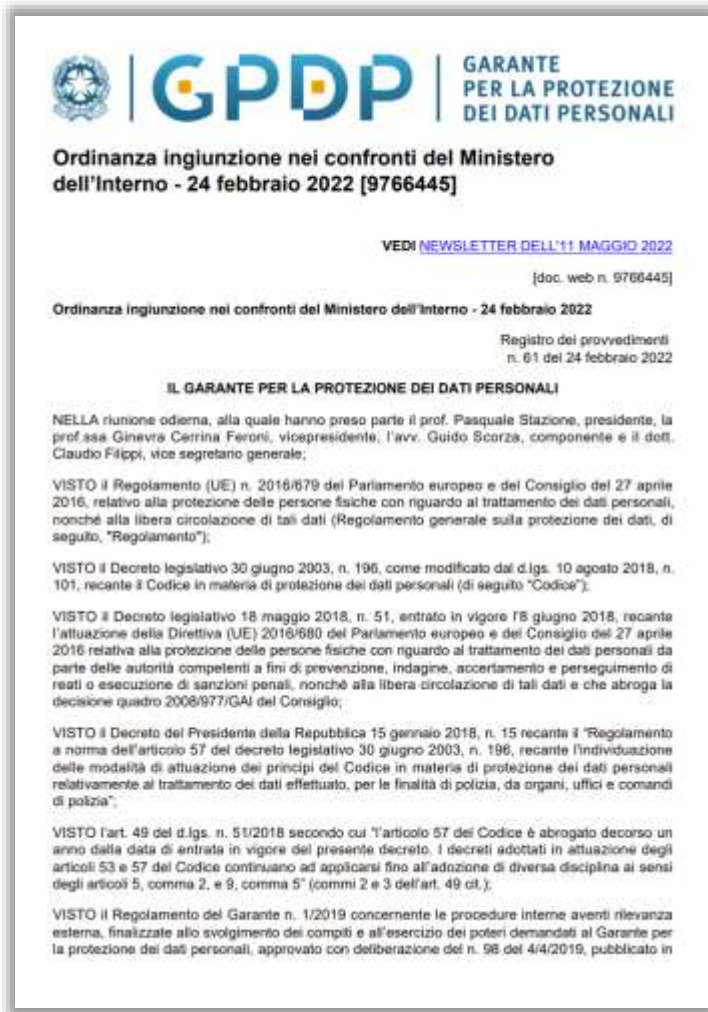
**Когда:** 2022.04

**За что:** нарушение ст. 58(2)(d) GDPR

**Как:** штраф €600

**Причина:** компании в декабре 2021г. AEPD вынесло предупреждение и предписание о принятии мер по предоставлению уведомлений о конфиденциальности (Privacy Notice) субъектам данных в соответствии со ст.13 GDPR. Компания у установленный срок предписание не выполнила и была оштрафована.

## Штраф за неосуществление DPIA и неинформирование о видеонаблюдении в общественных местах



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** муниципалитет Таранто

**Когда:** 2022.04

**За что:** нарушение ст. 5, 12, 13, 14, 28, 35 GDPR

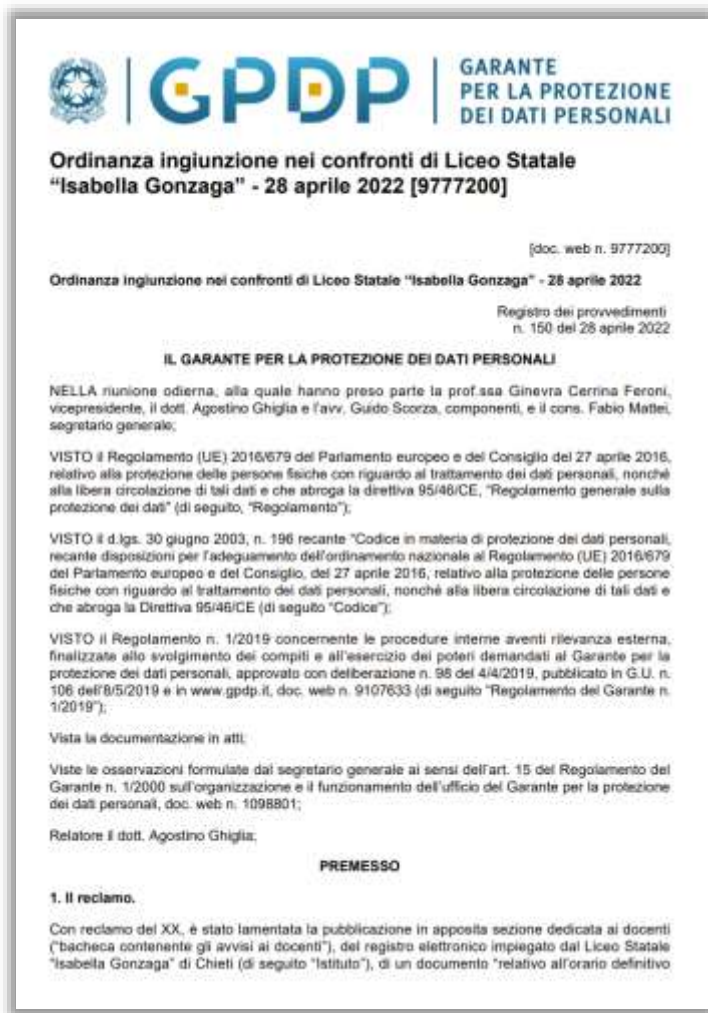
**Как:** штраф €150,000

**Причина:** Amiu s.p.a., как организация, ответственная за сбор отходов в муниципалитете, установила по запросу местных властей ряд камер видеонаблюдения с целью выявления и пресечения противоправного поведения, а жители муниципалитета не были проинформированы об этом.

Муниципалитет не урегулировал отношения с компанией Amiu, которая действовала в качестве обработчика данных, до начала операций по обработке.

Муниципалитет также не провел оценку воздействия на защиту данных ("DPIA"), которая была необходима.

## Штраф за непреднамеренное распространение чувствительных сведений о преподавательском составе



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Liceo Statale "Isabella Gonzaga"

**Когда:** 2022.04

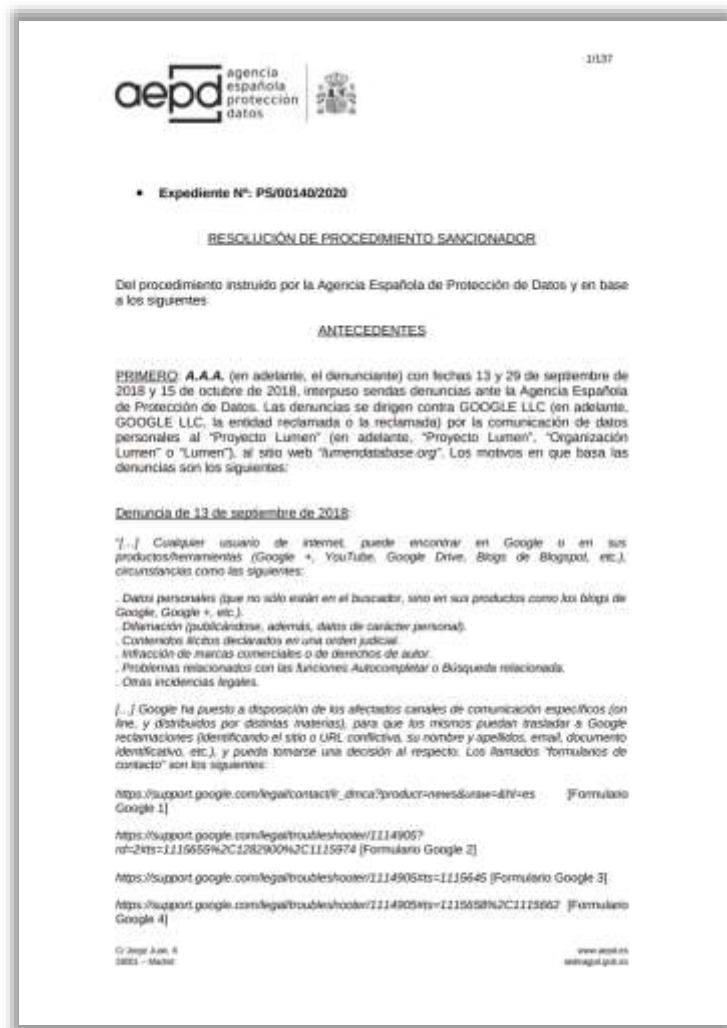
**За что:** нарушение ст. 5(1)(a), 5(1)(c), 6, 9 GDPR

**Как:** штраф €2,500

**Причина:** школа опубликовала в специальном разделе электронного реестра, предназначенном для учителей, документ, касающийся окончательного расписания на 2020-2021 учебный год, в котором рядом с именем одного из преподавателей была ссылка на льготы, полученные им в связи с инвалидностью.

Кроме того, данный документ содержал подробную информацию о личных и семейных событиях или информацию, связанную с конкретными трудовыми отношениями других учителей (например, декретный отпуск в связи с серьезными осложнениями беременности), и что данный документ был опубликован непреднамеренно – в результате человеческой ошибки.

## Штраф Google за незаконную передачу персональных данных и неспособность обеспечить право на их удаление



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Google LLC

**Когда:** 2022.05

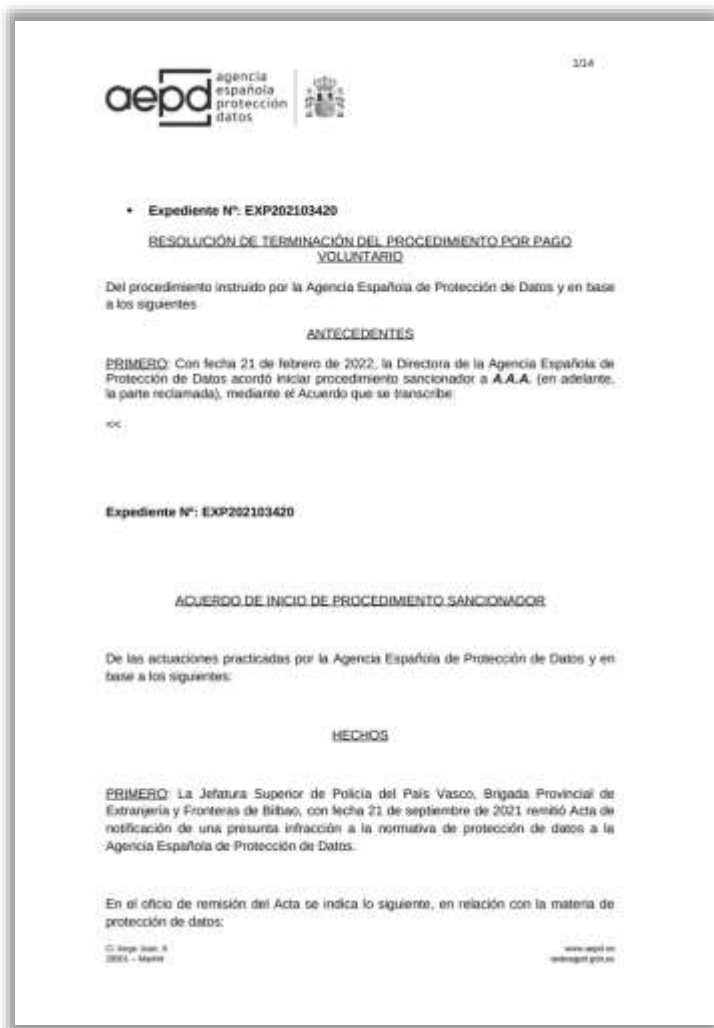
**За что:** нарушение ст. 6 и 17 GDPR

**Как:** штрафы €5,000,000 и €5,000,000

**Причина:** передача запросов, связанных с удалением контента из различных продуктов и платформ Google, таих как поисковая система Google и YouTube, третьей стороне – «Проекту Люмен» (Lumen Project). Для обеспечения возможности удаления контента Google требовал от пользователей, использовавших соответствующие формы, согласиться на передачу копий запросов на удаление контента на сайт lumendatabase.org, на котором они впоследствии публиковались. Что касается проекта Lumen, то его целью, как независимого исследовательского проекта, является изучение запросов на отзыв или удаление онлайн-контента, поступающих к интернет-издателям, поисковым системам и поставщикам услуг, содействие исследованию их различных типов, а также просвещение общественности.

Единственной информацией, предоставляемой пользователям о передаче персональных данных проекту Lumen, было уведомление в формах для подачи запроса, согласно которому Google передает в Lumen только анонимизированные контактные данные пользователя.

## 869 Штраф за несоблюдение принципа прозрачности



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** неназванная компания

**Когда:** 2022.05

**За что:** нарушение ст. 13 GDPR

**Как:** штрафы €500,000

**Причина:** после жалобы Высшего полицейского управления Страны Басков было начато расследование в отношении неназванной компании, чьи клиенты были вынуждены предоставить свои данные (как в письменном виде, так и путем предоставления копии документации), чтобы зарезервировать место на прием для обработки документации от Национальной полиции. Кроме того, неназванная компания не предоставила своим клиентам всю информацию, предусмотренную GDPR.

## 870 Штраф за нарушение правил использования файлов cookie



**Кто:** l'Autorité de protection des données (Бельгия)

**Кого:** Roularta Media Group

**Когда:** 2022.05

**За что:** нарушение ст. 4(11), 5(1)(e), 5(2), 6(1), 6(1)(a), 7(1), 7(3), 12(1), 13, 14, 24 GDPR

**Как:** штраф €50,000 + 3 месяца на исполнение предписания

**Причина:** согласие на обработку персональных данных посредством использования файлов cookie на сайтах levif.be и knack.be, управляемых компанией Roularta, не может считаться действительным. До получения согласия на пользовательских устройствах размещались файлы cookie, которые не были строго необходимы (например, статистические cookie).

Кроме того, согласие на использование cookies третьих лиц было неоднозначным из-за использования предварительно установленных флажков, и что согласие не может быть отозвано так же легко, как оно было предоставлено.

Политика конфиденциальности Roularta содержала недостаточную информацию об использовании cookies, сами cookies хранились неоправданно долго, а компания не соблюдала требование о предоставлении субъектам данных возможности отозвать свое согласие.

## Штраф за нарушение принципа минимизации данных при мониторинге действий работников



**Кто:** Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Persona (Румыния)

**Кого:** Mayr Melnhof Packaging Romania S.R.L.

**Когда:** 2022.05

**За что:** нарушение ст. 5(1)(b), 5(1)(c), 5(2), 6 GDPR

**Как:** штраф €15,000

**Причина:** компания установила систему видеонаблюдения, часть которой вела наблюдение за обеденной зоной и местом для курения на рабочем месте.

Таким образом, компания осуществляла чрезмерное наблюдение за работниками, выходящее за рамки заявленной цели, то есть обеспечения здоровья и безопасности работников, а также сохранности имущества.

Кроме того, полученные видеозаписи не обрабатывались надлежащим, релевантным и ограниченным образом для достижения заявленных целей.

## 872 Штраф за предоставление доступа к резюме без законного основания



**Kto:** Datatilsynet (Norge)

**Kogo:** Норвежское управление труда и благосостояния ('NAV')

**Kogda:** 2022.05

**Za chto:** нарушение ст. 5(1)(a), 5(1)(f), 6(1) GDPR

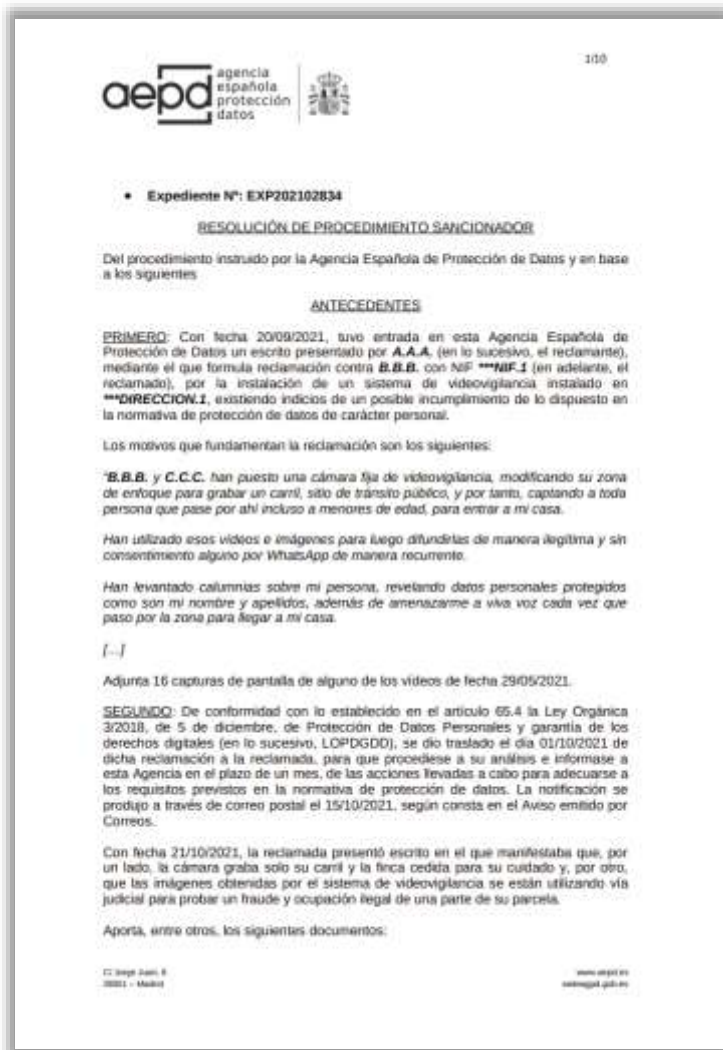
**Kak:** возможный штраф €485,000

**Причина:** для получения услуг по поиску работы и пособий кандидаты должны предоставить информацию, в том числе в форме резюме, которое быть доступно работодателям на сайте arbeidsplassen.no. Резюме содержали различные виды информации о зарегистрированных соискателях, такие как имя, место жительства, дата рождения, номер телефона, адрес электронной почты, образование, опыт работы и водительские права.

Было установлено, что NAV не располагало надлежащим правовым основанием для такого раскрытия данных кандидатов. Всего пострадало более 1,8 млн человек. NAV принял незамедлительные меры и закрыл работодателям доступ к просмотру резюме соискателей, а также проинформировал кандидатов.



## Штраф на физическое лицо за несоблюдение принципа минимизации данных



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** неназванное физическое лицо

**Когда:** 2022.06

**За что:** нарушение ст. 5(1)(с) GDPR

**Как:** штраф €300

**Причина:** нарушитель установил систему видеонаблюдения на своей ферме, которая запечатлела часть подъездной дороги общего пользования и въезд на соседнюю ферму.

## Штраф за использования «implicit opt-in» согласия на обработку файлов cookie



**Кто:** l'Autorité de protection des données (Бельгия)

**Кого:** Groupe Rossel

**Когда:** 2022.06

**За что:** нарушение ст. 6(1)(a), 7(3), 12(1), 13, 14 GDPR

**Как:** штраф €50,000

**Причина:** Groupe Rossel незаконно получила согласие пользователей на использование необязательных (аналитических, маркетинговых и т.д.) файлов cookie, применяя метод "дальнейшего просмотра", при котором было объединено выражение согласия пользователей на использование файлов cookie с выбором продолжения посещения сайта (implicit opt-in согласие).

Кроме того, на веб-сайтах продолжалась обработка необязательных файлов cookie после отзыва согласия пользователями, а политика Groupe Rossel в отношении файлов cookie на соответствующих веб-сайтах была неполной, поскольку не включала обязательную информацию о названиях всех ее сторонних партнеров, и не была представлена в достаточно доступной форме.

## Штраф за непреднамеренное распространение медицинских данных на веб-сайте



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Управление здравоохранения Рима

**Когда:** 2022.06

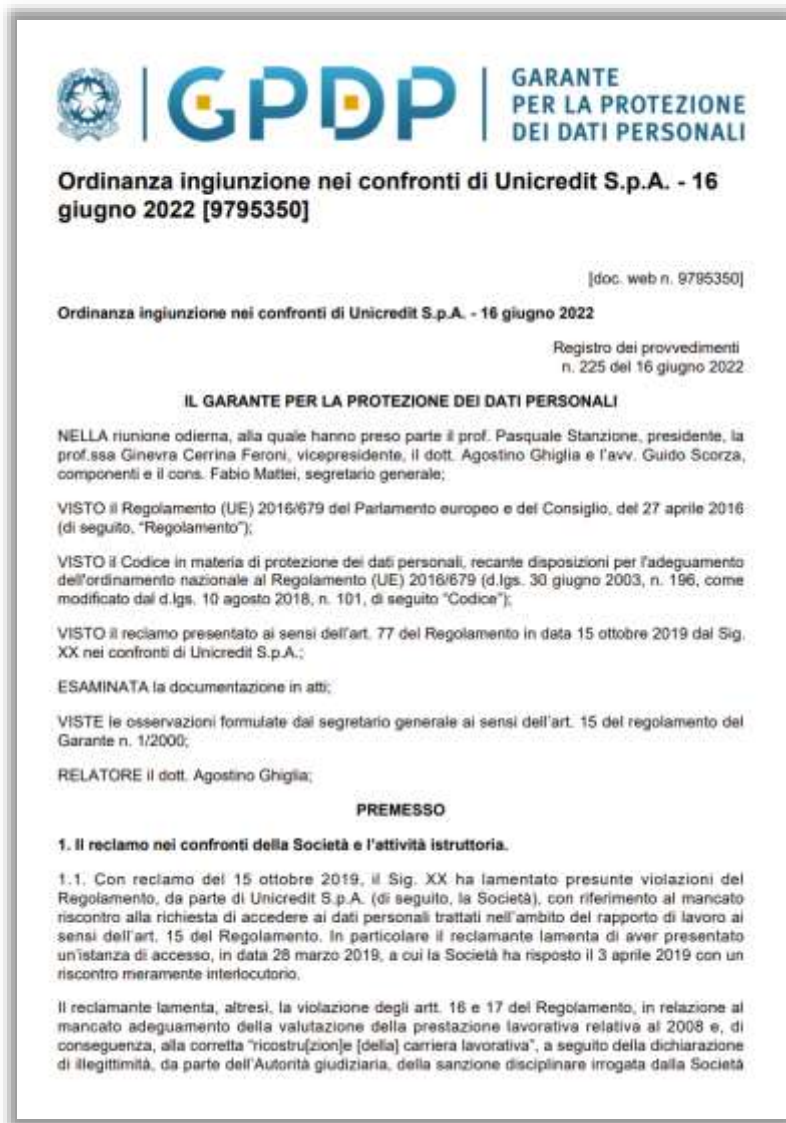
**За что:** нарушение ст. 5(1)(c), 6(1)(c), 6(1)(e), 6(2), 6(3)(b), 9(1), 9(2), 9(4) GDPR

**Как:** штраф €46,000

**Причина:** управление здравоохранения опубликовало на своем веб-сайте открытым текстом имена и медицинские данные лиц, которые в период с 2017 по 2018 год запрашивали доступ к медицинским документам, таким как медицинские карты, оценки инвалидности, результатам лабораторных анализов.

При определении размера штрафа были приняты во внимание смягчающие факторы, такие как случайный характер действий, отсутствие жалоб от заинтересованных субъектов данных и своевременные действия контролера по устранению нарушения.

## Штраф за непреднамеренное распространение медицинских данных на веб-сайте



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** UniCredit S.p.A.

**Когда:** 2022.06

**За что:** нарушение ст. 12, 15 GDPR

**Как:** штраф €70,000

**Причина:** UniCredit не удовлетворил запрос заявителя на доступ к его данным, т.к. заявитель не заполнил форму запроса данных на портале конфиденциальности банка.

ДРА ответил, что применение формы запроса на доступ к данным может представлять собой организационную модальность, направленную на содействие заинтересованным субъектам данных, но не должна быть условием действительного запроса.

## Штраф за незаконное видеозаписи для анализа ошибок системы помощи водителю

Presse



Die Landesbeauftragte für den  
Datenschutz Niedersachsen

26.07.2022

### Datenschutzverstöße im Rahmen von Forschungsfahrten 1,1 Millionen Euro Bußgeld gegen Volkswagen

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen hat gegen die Volkswagen Aktiengesellschaft eine Geldbuße nach Art. 83 Datenschutz-Grundverordnung (DS-GVO) in Höhe von 1,1 Millionen Euro festgesetzt. Grund sind Datenschutzverstöße in Zusammenhang mit dem Einsatz eines Dienstleisters bei Forschungsfahrten für ein Fahrassistenzsystem zur Vermeidung von Verkehrsunfällen. Das Unternehmen hat umfassend mit der LfD Niedersachsen kooperiert und den Bußgeldbescheid akzeptiert.

Ein Erprobungsfahrzeug des Unternehmens wurde im Jahr 2019 durch die österreichische Polizei bei Salzburg für eine Verkehrskontrolle angehalten. Den Polizeibediensteten waren am Fahrzeug ungewöhnliche Anbauten aufgefallen, die sich noch vor Ort als Kameras herausstellten. Das Fahrzeug wurde eingesetzt, um die Funktionsfähigkeit eines Fahrassistenzsystems zur Vermeidung von Verkehrsunfällen zu testen und zu trainieren. Unter anderem zur Fehleranalyse wurde das Verkehrsgeschehen um das Fahrzeug herum aufgezeichnet.

Am Fahrzeug fehlten aufgrund eines Versehens Magnetschilder mit einem Kamerasymbol und den weiteren vorgeschriebenen Informationen für die datenschutzrechtlich Betroffenen, in diesem

**Kontakt:**  
Die Landesbeauftragte für den  
Datenschutz Niedersachsen  
Presse Sprecher  
Johannes Pepping  
Tel.: 0511 120-4551

Internet: [www.lfd.niedersachsen.de](http://www.lfd.niedersachsen.de)  
E-Mail: [pressestelle@lfd.niedersachsen.de](mailto:pressestelle@lfd.niedersachsen.de)  
Postanschrift:  
Prinzenstr. 5, 30159 Hannover

**Кто:** LfD Niedersachsen (Германия)

**Кого:** Volkswagen AG

**Когда:** 2022.07

**За что:** нарушение ст. 13, 28, 30, 35 GDPR

**Как:** штраф €1,100,000

**Причина:** в 2019г. австрийская полиция остановила тестовый автомобиль компании Volkswagen, после чего полицейские заметили на автомобиле необычные приспособления, которые оказались камерами. Автомобиль использовался для тестирования и обучения функциональности системы помощи при вождении для предотвращения ДТП, а движение вокруг тестового автомобиля записывалось для анализа ошибок.

Надзорный орган установил следующие нарушения GDPR:

- ◇ по недосмотру на тестовом автомобиле отсутствовали информационные знаки, которые должны были быть установлены в соответствии со ст.13;

- ◇ Volkswagen не заключил соглашение об обработке данных с компанией, которая проводила тест-драйвы, тем самым нарушив ст.28;

- ◇ в RoPA отсутствовало описание технических и организационных мер безопасности, что привело к нарушению требований ст.30;

- ◇ не была проведена оценка воздействия на защиту данных (DPIA) в соответствии со ст.35.

## Штраф за незаконное профилирование клиентов банка в рекламных целях в рамках Legitimate interest



**Кто:** LfD Niedersachsen (Германия)

**Кого:** неназванный банк

**Когда:** 2022.07

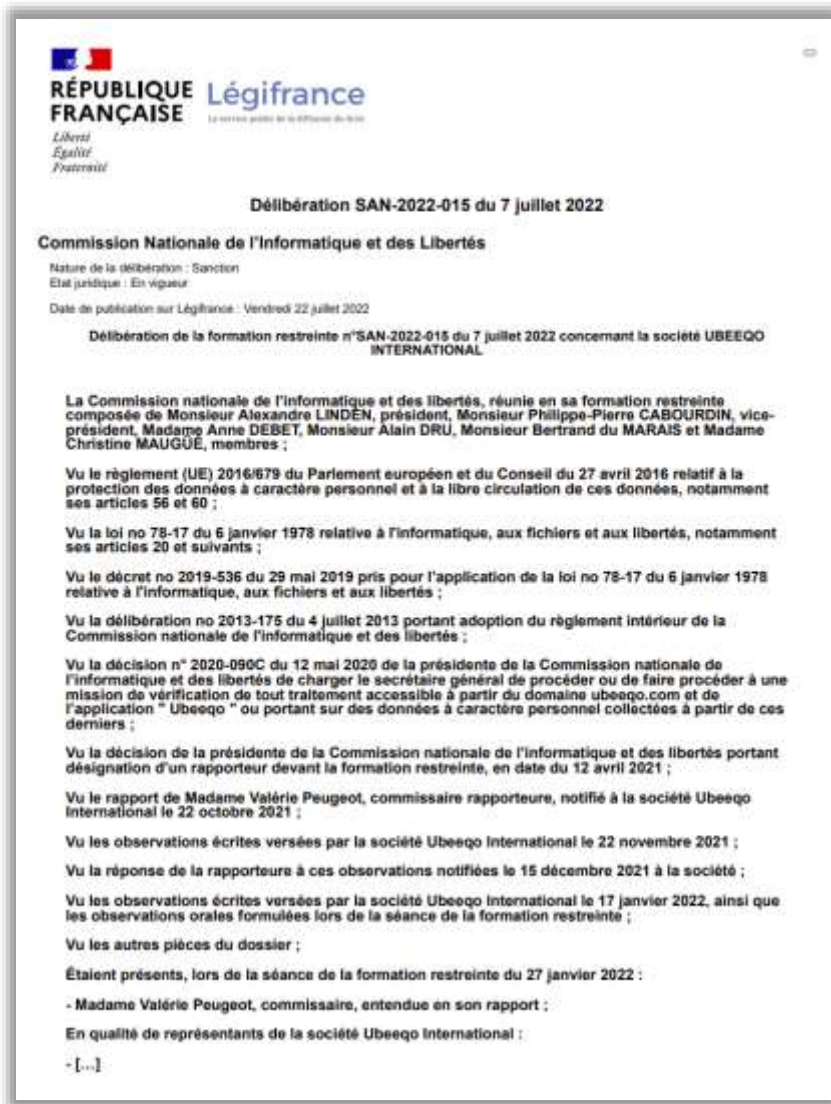
**За что:** нарушение ст.6 GDPR

**Как:** штраф €900,000 и запрет на создание рекламных профилей и оптимизации на основе действий и атрибутов пользователя в рамках законного интереса банка

**Причина:** банк проанализировал данные активных и бывших клиентов (общий объем покупок в магазинах приложений, частота использования принтеров для печати выписок и общая сумма переводов). Результаты анализа сравнивались с данными кредитного агентства и обогащались на их основе. Цель состояла в том, чтобы выявить клиентов с большей склонностью к цифровым медиа и более эффективно работать с ними.

DPA указал, что законный интерес контролера данных нельзя использовать для легализации профилирования, поскольку субъекты не ожидают, что контролеры данных будут использовать файлы данных в больших масштабах, чтобы определить их склонность к определенным категориям продуктов или каналам коммуникации.

## Штраф на процессора за непропорциональную геолокацию арендованных автомобилей



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** UBEEQO International

**Когда:** 2022.07

**За что:** нарушение ст.5(1)(c), 5(1)(e), 12 GDPR

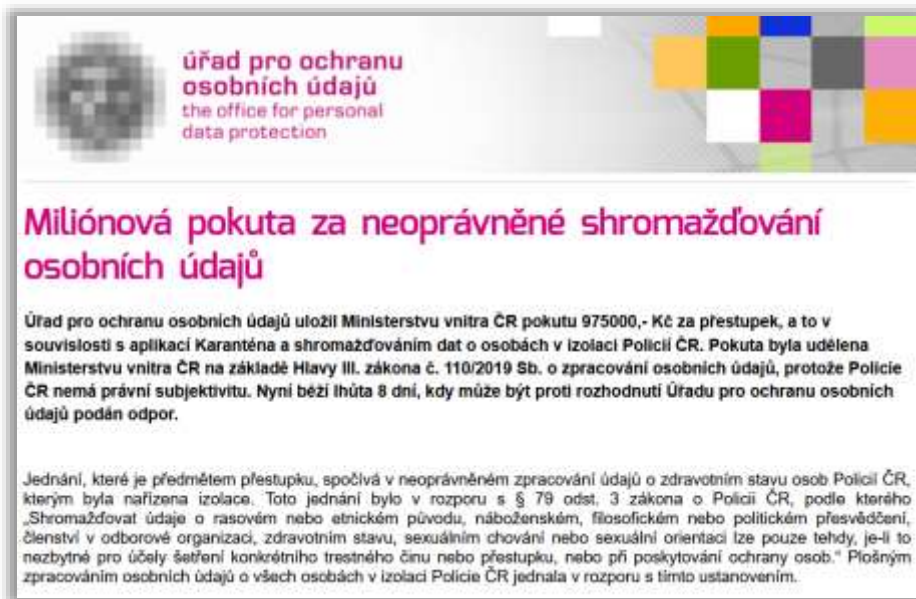
**Как:** штраф €175,000

**Причина:** CNIL провела расследование в отношении компании UBEEQO INTERNATIONAL, которая сдает автомобили в аренду на короткий срок. Компания собирала данные о геолокации (с частотой каждые 500 метров) своих автомобилей, сдаваемых в аренду каждые 500 метров.

Цели компании (обслуживание и предоставление услуг, определение местоположения в случае кражи, помощь клиентам) не оправдывают сбор данных о геолокации.

Период хранения указанных данных в 3 года и более является необоснованно большим. Кроме того, компания хранила данные пользователей, которые были неактивны более 8 лет, хотя учетные записи неактивных пользователей необходимо регулярно удалять.

## Штраф за незаконный сбор данных о лицах, находящихся на обязательной изоляции в период пандемии



**Кто:** Úřad pro ochranu osobních údajů (Чехия)

**Кого:** Министерство внутренних дел Чешской Республики

**Когда:** 2022.07

**За что:** нарушение ст. 5, 6 GDPR

**Как:** штраф €40,000

**Причина:** сбор персональных данных о людях, находящихся на обязательной изоляции в период пандемии. По Закону о полиции Чешской Республики такие конфиденциальные данные могут собираться только в том случае, если это необходимо для расследования конкретного преступления или проступка, или для предоставления защиты лицам.

Президиум полиции начал получать персональные данные людей, находящихся на карантине после контакта с инфицированным или в изоляции после заражения во время вспышки эпидемии Covid-19 два года назад. Распоряжение об этом в конце марта 2020 года отдала районным гигиеническим станциям занимавшая в то время должность главного санэпидемврача Ярмила Ражова.



## Штраф за раскрытие медицинских данных и неисполнение предписания надзорного органа

### PENALTY NOTICE

Given to: **Manx Care**  
Head Office  
Noble's Hospital Estate  
Strang  
BRADDAN  
Isle of Man  
IM4 4RU

Date: **13 July 2022**

1. In this penalty notice:
  - a. "Article" means an article of the Applied GDPR
  - b. "Applied GDPR" means the Annex to the Data Protection (Application of GDPR) Order 2018
  - c. "Implementing Regulations" means the GDPR and LED Implementing Regulations 2018
  - d. "Regulation" means a regulation of the Implementing Regulations
  - e. "Notice of Intent" means the 'notice of intent to give the penalty notice' given in accordance with Regulation 112(4) and Schedule 5 to the Implementing Regulations
2. The Information Commissioner ("**the Commissioner**"), pursuant to Regulation 112(1) of and Paragraph 2 of Schedule 5 to, the Implementing Regulations, has decided to give a penalty notice to Manx Care.
3. Manx Care is the 'controller' as defined in Article 4(7).
4. This penalty notice ("**Notice**") imposes an administrative fine on Manx Care, in accordance with the Commissioner's powers under Article 83 of the Applied GDPR.
5. The amount of the penalty is **£170,500.00** (One Hundred and Seventy Thousand and Five Hundred Pounds). Payment of the penalty is subject to paragraphs 35 and 36.
6. This Notice explains the Commissioner's reasons for imposing the penalty and the amount of the penalty, including any aggravating or mitigating factors taken into account.

**Кто:** Information Commissioner (Остров Мэн)

**Кого:** Manx Care Limited

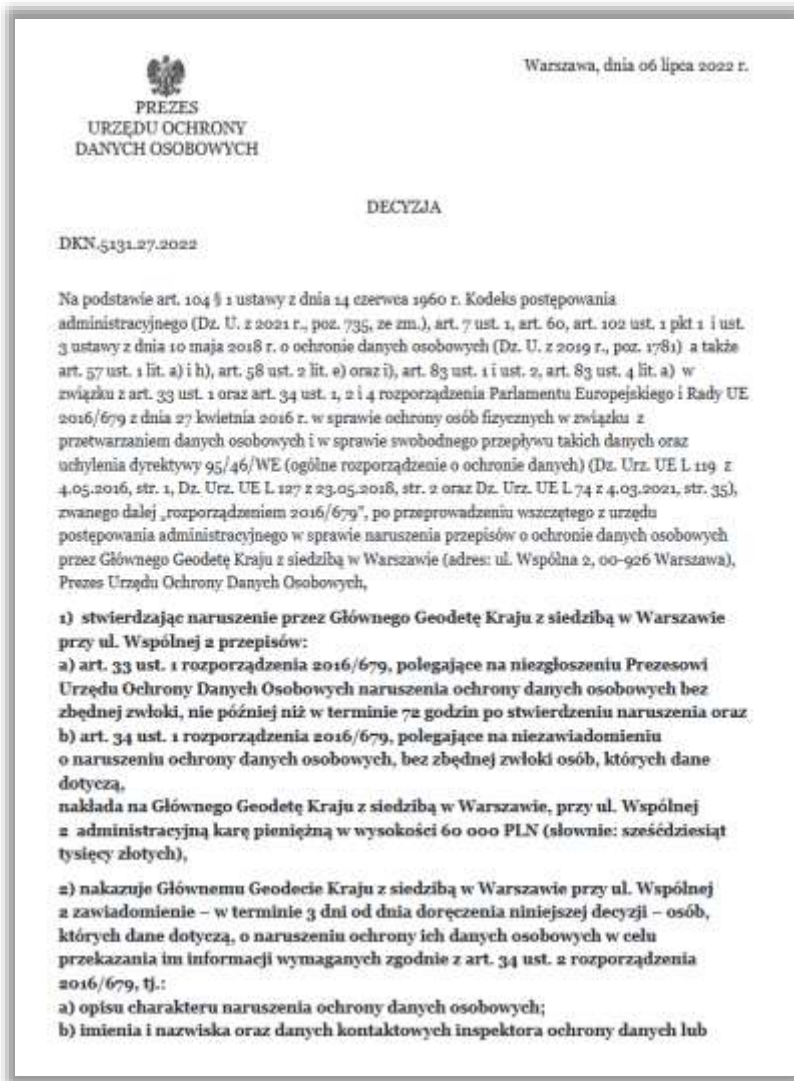
**Когда:** 2022.07

**За что:** нарушение ст. 5(1)(с), 5(1)(f), 5(2), 24, 25, 32, 34, 58 GDPR

**Как:** штраф £170,500

**Причина:** в октябре 2021 года компания Manx Care отправила по электронной почте 1,870 различным получателям незащищенное вложение, содержащее конфиденциальные медицинские данные одного из пациентов. Позднее, компания не смогла выполнить предписание Комиссара по информации от [25.02.2022](https://www.inforights.im/organisations/latest-news-updates/2022/aug/penalty-imposed-on-manx-care/).

## Штраф за неуведомление о нарушении безопасности персональных данных



**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** Генеральный инспектор Польши по геодезии (GGK)

**Когда:** 2022.07

**За что:** нарушение ст. 33(1), 34(1) GDPR

**Как:** штраф €12,600

**Причина:** в апреле 2022г. номера земельных и ипотечных регистров стали общедоступны в течение более 48 часов в сервисе, обслуживаемом Генеральным геодезистом Польши, т.е. [www.geoport.gov.pl](http://www.geoport.gov.pl). По номеру земельного и ипотечного регистра легко определить ряд данных владельцев недвижимости, включая, в частности, их личные идентификационные номера (номера PESEL), имена и фамилии, имена родителей и адрес недвижимости.

Польский надзорный орган (SA) узнал о нарушении безопасности персональных данных не от контролера, который должен был уведомить об этом надзорный орган, а из СМИ.

В ходе разбирательства GGK утверждал, что номера земельных и ипотечных регистров не являются персональными данными, что являются доступными на других сервисах, а кратковременное появление номеров на сайте [www.geoport.gov.pl](http://www.geoport.gov.pl) не привело к какому-либо риску для прав и свобод физических лиц.

## Штраф за непреднамеренное раскрытие медицинских данных в электронном письме



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Senseonics Inc.

**Когда:** 2022.07

**За что:** нарушение ст. 5(1)(a)(b)(f), 6, 7, 9, 12, 13, 27 GDPR

**Как:** штраф €45,000

**Причина:** работник компании случайно добавил ненадлежащих получателей электронной почты в копию письма и тем самым раскрыл информацию о состоянии здоровья каждого получателя. Что еще более интересно, штраф наложен не только за раскрытие информации, но и за неправильный механизм сбора согласия - один флажок отвечал за несколько целей обработки.

# Штраф за несоблюдение прав субъектов данных при обработке их запросов

**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

**Кого:** Otavamedia Oy

**Когда:** 2022.07

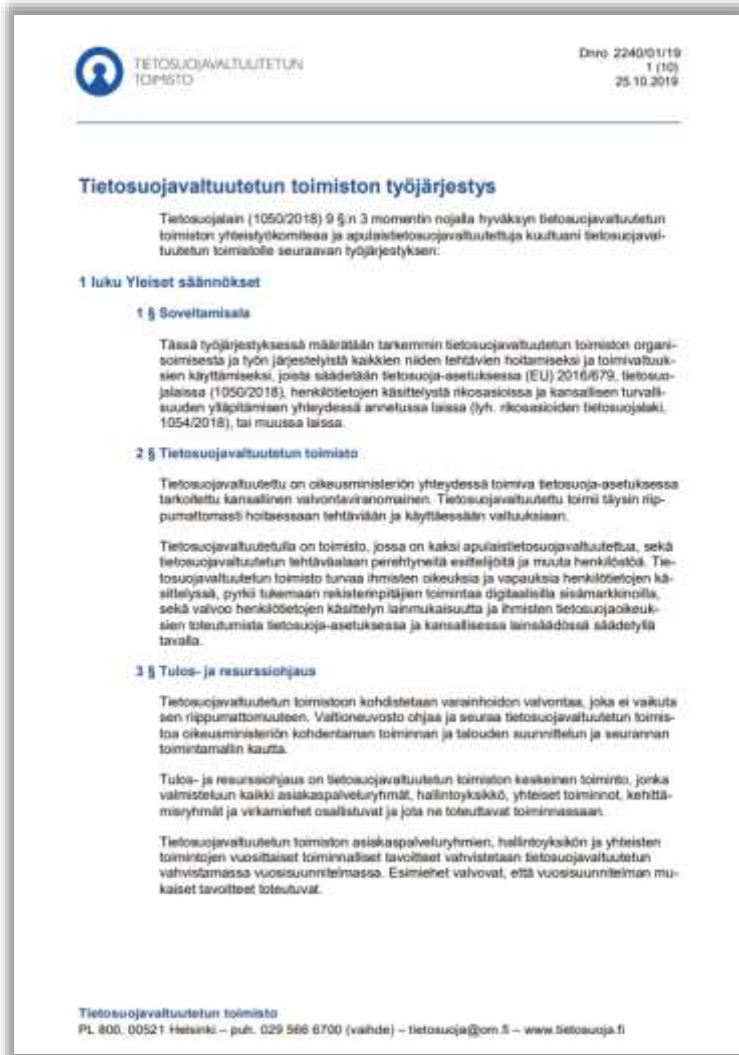
**За что:** нарушение ст. 5(1)(c), 12, 15, 17, 25 GDPR

**Как:** штраф €85,000

**Причина:** надзорный орган в период 2018-2021 годов получил 11 жалоб на обработку персональных данных компанией, в том числе в связи с непредоставлением ответов на запросы субъектов данных.

Согласно объяснениям компании, ответы на некоторые запросы субъектов данных не были получены из-за технических проблем с контролем электронной почты в связи со сменой поставщика услуг. Сама проблема была обнаружена компанией только после получения просьбы о разъяснении со стороны надзорного органа, и что проблемы с электронной почтой продолжались в течение семи месяцев.

Кроме того, субъекты данных могли направлять запросы в компанию с помощью типовой бумажной формы, которая требовала подписи субъекта в целях его идентификации. В результате этого был собран неоправданно большой объем данных, так как у компании отсутствовала возможность подтвердить достоверность подписей в полученных запросах путем их сравнения с иными образцами подписей субъектов.





**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Accor SA

**Когда:** 2022.08

**За что:** нарушение ст. 12, 13, 15, 21, 32 GDPR и ст. L.34-5 Кодекса почтовых и электронных коммуникаций Франции

**Как:** штраф €600,000

**Причина:** лица, бронирующие номера непосредственно в Accor или в одном из брендов, входящих в ее группу, автоматически добавляются в список получателей информационного бюллетеня, содержащего коммерческие предложения, благодаря предварительно установленному флажку, дающему согласие на это. Кроме того, технические проблемы не позволили людям воспользоваться своим правом на возражение против получения прямых маркетинговых сообщений.

Контролер также продемонстрировал неспособность отвечать на запросы субъектов данных о доступе к данным в требуемые сроки и неспособность обеспечить безопасность персональных данных, поскольку допускалось использование клиентами небезопасных паролей.

## Штраф за нарушения в длительности хранения и безопасности персональных данных



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** G.I.E. Infogreffe

**Когда:** 2022.09

**За что:** нарушение ст. 5(1)(e), 32 GDPR

**Как:** штраф €250,000

**Причина:** надзорный орган, после получения жалобы, провел онлайн-инспекцию сайта infogreffe.fr, который позволяет пользователям получать юридическую информацию о компаниях и заказывать документы, заверенные реестрами коммерческих судов.

CNIL установила, что личные данные (включая банковские реквизиты, фамилии, имена, почтовые и электронные адреса) 25% пользователей сервиса хранились дольше срока, определенного G.I.E. Infogreffe (т.е. 36 месяцев с момента последнего заказа услуги и/или документа).

Компания не требовала использования надежного пароля при создании учетной записи на своем сайте. Кроме того, G.I.E. Infogreffe передавала открытым способом по электронной почте пароли, позволяющие получить доступ к учетным записям, а также хранила без шифрования в своей базе данных пароли, секретные вопросы и ответы, которые использовались пользователями во время процедуры сброса пароля.

## 887 Штраф на Instagram за нарушение в обработке данных детей



**Кто:** Data Protection Commission (Ирландия)

**Кого:** Instagram

**Когда:** 2022.09

**За что:** нарушение ст. 5(1)(a), 5(1)(c), 6(1), 12(1), 24, 25(1), 25(2), 35(1) GDPR

**Как:** штраф €405,000,000

**Причина:** Расследование началось ещё в 2020 году. Instagram позволял подросткам 13-17 лет настраивать бизнес-аккаунты, что делало их контактную информацию общедоступной. Во-вторых, соцсеть сделала аккаунты некоторых молодых пользователей общедоступными по умолчанию.

Ирландский регулятор завершил работу над проектом итогового постановления по расследованию Instagram в декабре 2021 года. Он поделился им с другими регулирующими органами Европейского союза в рамках системы «единого окна» для регулирования деятельности крупных транснациональных корпораций.

Instagram обновил свои настройки более года назад и с тех пор выпустил новые функции для обеспечения безопасности подростков и конфиденциальности их информации. Instagram не согласен с тем, как был рассчитан штраф, и будет добавиться пересмотра решения.

## Штраф за незаконное получение и обработку данных из электронного земельного кадастра



**Кто:** LfDI Baden-Württemberg (Германия)

**Кого:** неназванный застройщик и геодезист

**Когда:** 2022.09

**За что:** нарушение ст.6(1), 14 GDPR

**Как:** штраф €50,000 на компанию и €5,000 на геодезиста

**Причина:** владелец недвижимости в районе новой застройки получил письмо от компании, занимающейся застройкой, с предложением о цене покупки его недвижимости. В письме не было никакой информации о происхождении данных владельца недвижимости.

Ранее геодезист воспользовался своими полномочиями для проверки электронного земельного кадастра, выявил несколько сотен владельцев недвижимости без их ведома и передал соответствующую информацию компании-застройщику, которая, в свою очередь, связалась с владельцами недвижимости.

Кроме того, владельцам недвижимости не была предоставлена информация об обработке их данных, даже когда с ними связывалась компания, что является нарушением ст.14 GDPR.



### Pressemitteilung

711.412.1

5. November 2019

#### Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft

Am 30. Oktober 2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) erlassen.

Bei Vor-Ort-Prüfungen im Juni 2017 und im März 2019 hat die Aufsichtsbehörde festgestellt, dass das Unternehmen für die Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendete, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen. Personenbezogene Daten von Mieterinnen und Mietern wurden gespeichert, ohne zu überprüfen, ob eine Speicherung zulässig oder überhaupt erforderlich ist. In begutachteten Einzelfällen konnten daher teilweise Jahre alte private Angaben betroffener Mieterinnen und Mieter eingesehen werden, ohne dass diese noch dem Zweck ihrer ursprünglichen Erhebung dienten. Es handelte sich dabei um Daten zu den persönlichen und finanziellen Verhältnissen der Mieterinnen und Mieter, wie z. B. Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankensicherungsdaten sowie Kontoauszüge.

Nachdem die Berliner Datenschutzbeauftragte im ersten Prüftermin 2017 die dringende Empfehlung ausgesprochen hatte, das Archivsystem umzustellen, konnte das Unternehmen auch im März 2019, mehr als eineinhalb Jahre nach dem ersten Prüftermin und neun Monate nach Anwendungsbeginn der Datenschutz-Grundverordnung weder eine Bereinigung ihres Datenbestandes noch rechtliche Gründe für die fortdauernde Speicherung vorweisen. Zwar hatte das Unternehmen Vorbereitungen zur Beseitigung der aufgefundenen Missstände getroffen. Diese Maßnahmen hatten jedoch nicht zur Herstellung eines rechtmäßigen Zustands bei der Speicherung personenbezogener Daten geführt. Die Verhängung eines Bußgeldes wegen eines

Pressesprecherin: Dalia Kues  
Geschäftsstelle: Cristina Vecchi  
E-Mail: [presse@datenschutz-berlin.de](mailto:presse@datenschutz-berlin.de)

Friedrichstr. 219    Tel: 030 13889 - 900  
10969 Berlin        Fax: 030 2156050



**Кто:** BDI Berliner (Германия)

**Кого:** дочерняя компания неназванной ритейл-группы

**Когда:** 2022.09

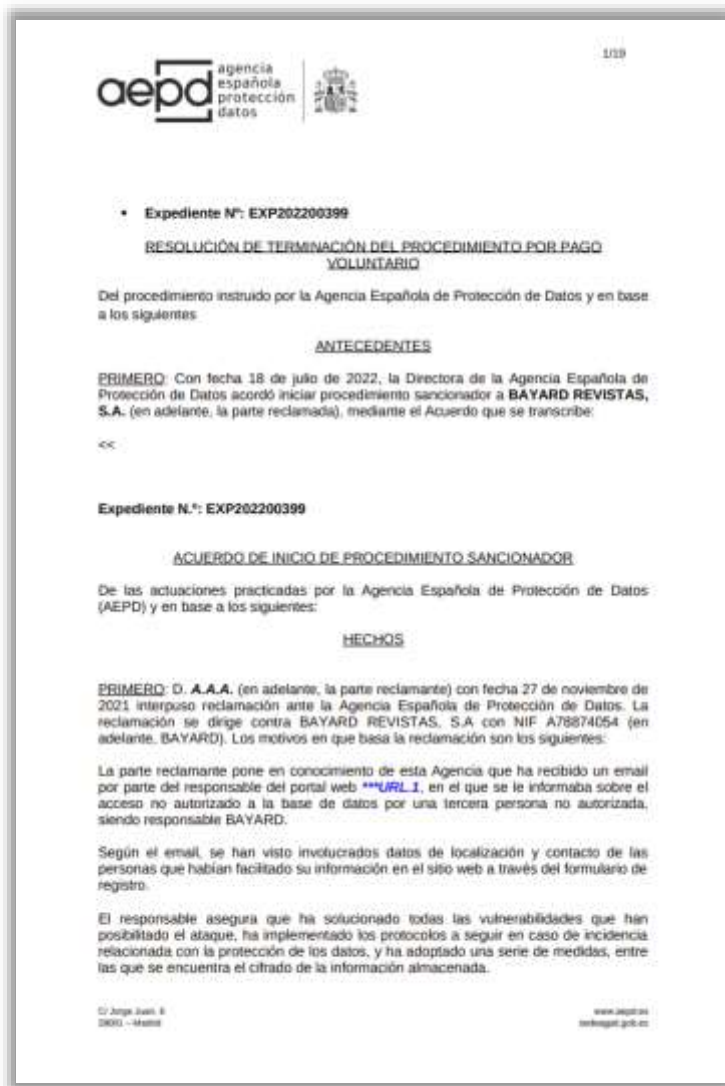
**За что:** нарушение ст.38(6) GDPR

**Как:** штраф €525,000 после первоначального предупреждения, вынесенного компании в 2021 году

**Причина:** компания назначила DPO для независимого контроля решений, принятых им же в другом качестве. Данное лицо являлось управляющим директором двух сервисных компаний в рамках одной группы, которые обрабатывали персональные данные от имени компании, для которой оно являлось DPO, при обслуживании клиентов и выполнении заказов.

В связи с этим DPA уточнил, что DPO должен был следить за соблюдением законодательства о защите данных сервисными компаниями, которыми он руководил как управляющий директор.

## Штраф за задержку в уведомлении о нарушении безопасности персональных данных



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Bayard Revistas S.A.

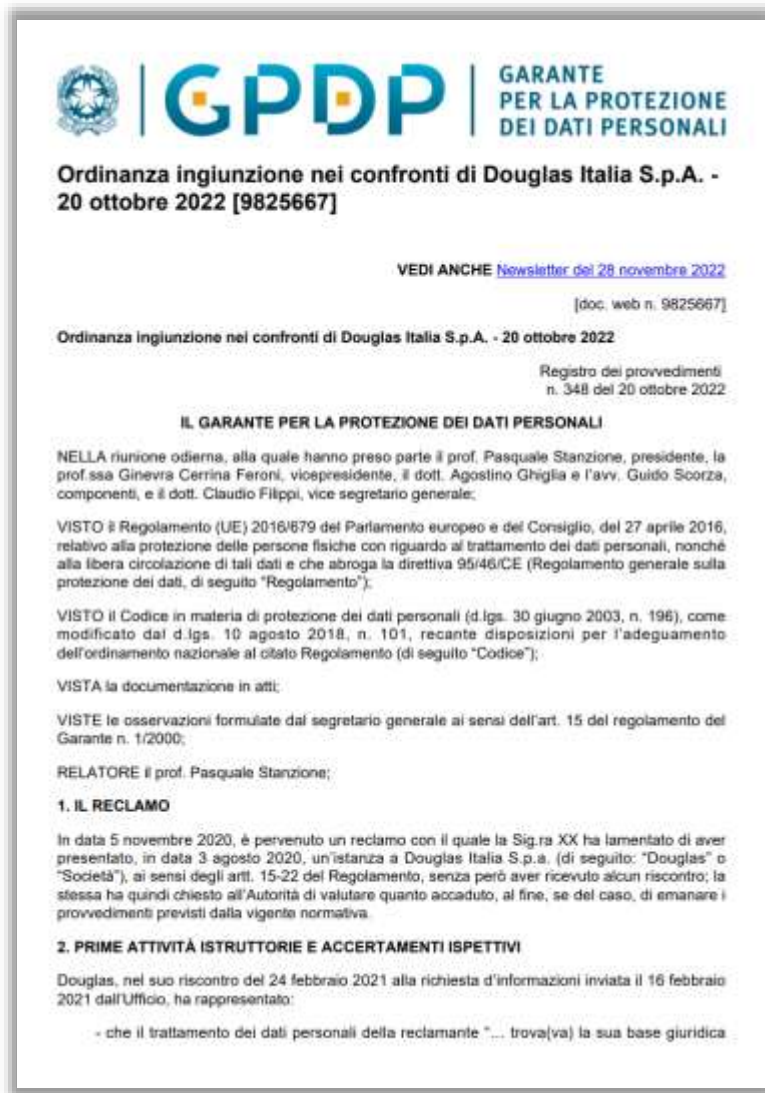
**Когда:** 2022.09

**За что:** нарушение ст. 5(1)(f), 32, 33 GDPR

**Как:** штраф €52,000, который был уменьшен до €31,200

**Причина:** пользовательские данные в базе данных сайта Bayard были незаконно раскрыты третьей стороне. Кроме того, компания Bayard как контролер данных не приняла надлежащих технических и организационных мер для обеспечения надлежащего уровня безопасности. Наконец, знала о нарушении безопасности 28.10.2021 и не сообщала AEPD об инциденте до 11.11.2021.

## Штраф за непреднамеренное раскрытие медицинских данных в электронном письме



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Douglas Italia S.p.A.

**Когда:** 2022.10

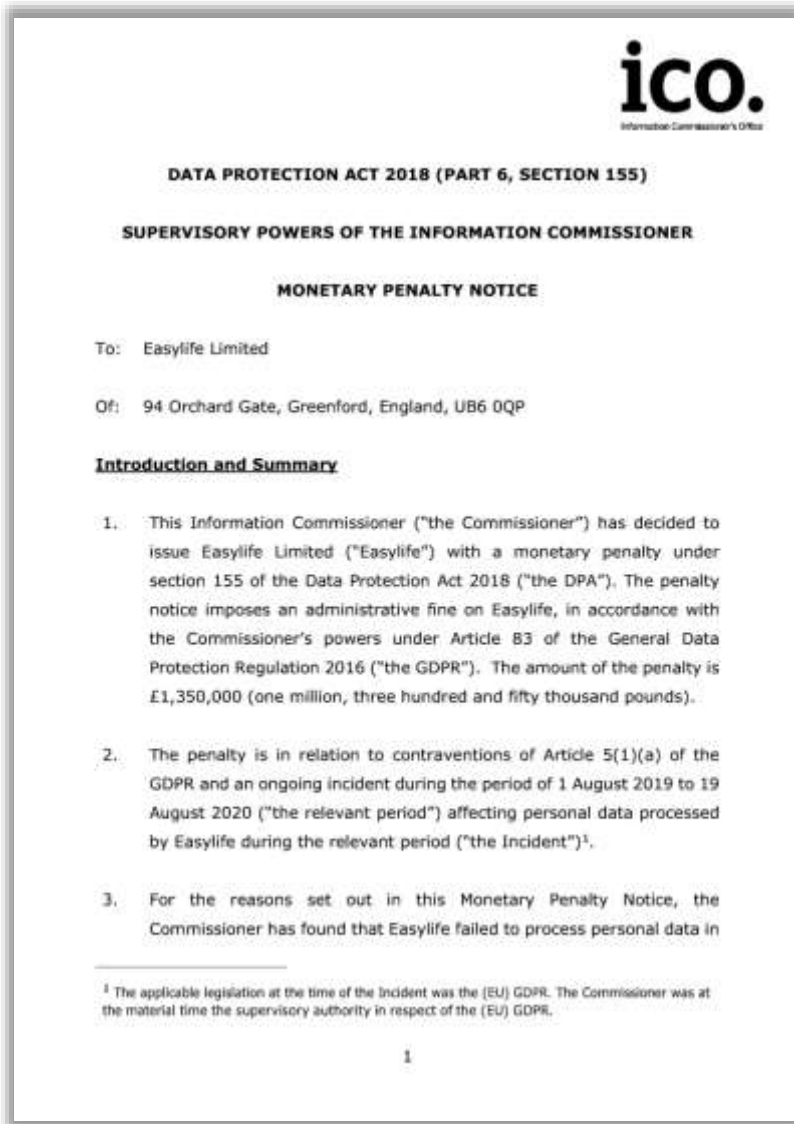
**За что:** нарушение ст. 5(1)(b), 5(1)(e), 5(2), 6, 7, 12(1), 13(2)(a), 24, 25(1) GDPR

**Как:** штраф €1,400,000

**Причина:** Douglas Italia была создана в результате слияния трех компаний-предшественников, а база данных Douglas Italia (содержащая около 10 миллионов клиентов) объединяет данные этих компаний. Среди выявленных нарушений было следующее:

1. требование от пользователей одновременного согласия с общими условиями продажи, уведомлением о конфиденциальности и политикой использования файлов cookie;
2. хранение в неактивном состоянии данных клиентов, которые не продлили свои карты верности в Douglas Italia, чтобы облегчить возможную замену карт лояльности;
3. клиенты, которые дали согласие только на телемаркетинг, получали также SMS маркетинговые сообщения, и наоборот.

## Штраф за незаконное профилирование и прогнозирование состояния здоровья



**Кто:** Information Commissioner's Office (Великобритания)

**Кого:** Easylife Ltd

**Когда:** 2022.10

**За что:** нарушение ст.5(1)(a) UK GDPR и п.21 Privacy and Electronic Communications Regulations 2003 ('PECR')

**Как:** штраф €1,540,000 за нарушение UK GDPR и €148,000 за нарушение PECR

**Причина:** компания использовала личную информацию 145,400 клиентов для прогнозирования их состояния здоровья и целевого предложения им товаров медицинского характера, без их согласия. Имело место значительное профилирование клиентов и обработка данных о здоровье, и что эти лица не знали о сборе и использовании их персональных данных в таких целях.

Что касается нарушений в рамках PECR, то за один год Easylife совершила 1,345,732 нежелательных маркетинговых звонка людям, зарегистрированным в Службе телефонных предпочтений, что запрещено PECR без согласия получателя.

## 893 Штраф за неадекватные меры безопасности данных после кибератаки



**Кто:** Information Commissioner's Office (Великобритания)

**Кого:** Interserve Group Limited

**Когда:** 2022.10

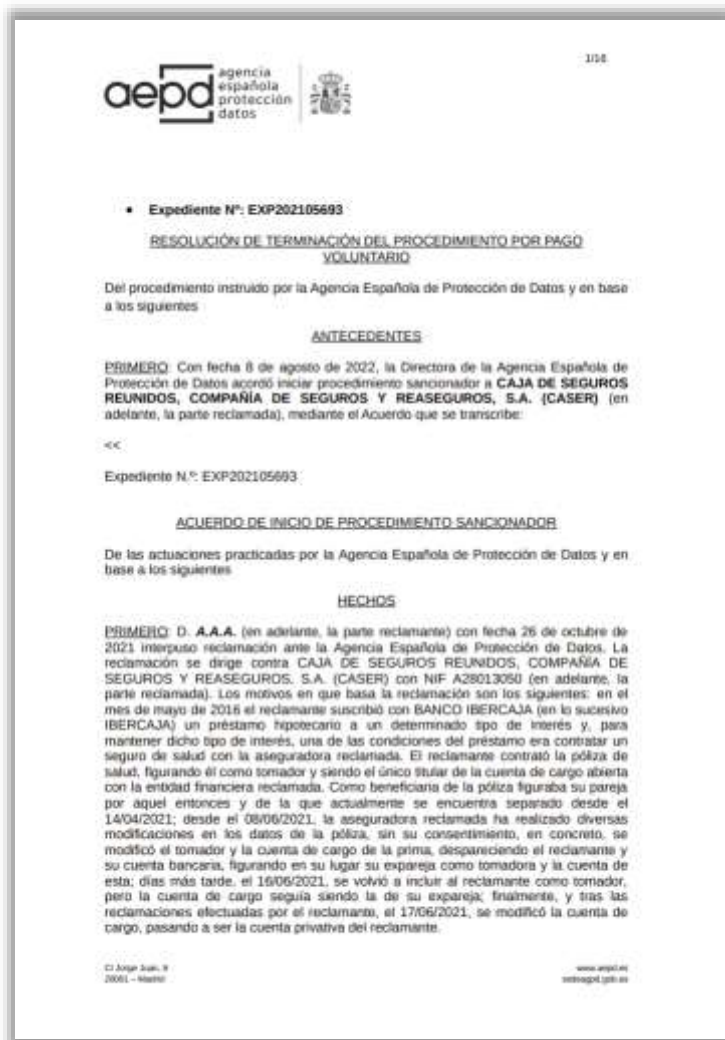
**За что:** нарушение ст. 5(1)(f), 32(1)(b), 32(1)(d) UK GDPR

**Как:** штраф €4,970,000

**Причина:** Interserve подверглась кибератаке после того, как на почтовый ящик команды бухгалтеров было отправлено фишинговое письмо, которое установило вредоносное ПО на рабочие станции и предоставило злоумышленнику доступ к персональным данным. Злоумышленник взломал серверы Interserve, на которых хранились персональные данные (номера телефонов, адреса электронной почты, номера национального страхования, данные банковских счетов, семейное положение, дата рождения, образование, страну рождения, пол, количество иждивенцев, информацию о контактах в чрезвычайных ситуациях и зарплату), в том числе конфиденциального характера, относящиеся к 113,000 человек. Среди выявленных нарушения было следующее:

- обработка персональных данных на неподдерживаемых операционных системах, которые больше не были предметом обновлений безопасности для устранения известных уязвимостей;
- отсутствие надлежащей защиты APM;
- отсутствие надлежащего и эффективного информационного обучения работников;
- отсутствие эффективного и своевременного расследования причин первоначальной атаки;
- неспособность эффективно управлять доступом к привилегированным учетным записям.

## 894 Штраф за изменение персональных данных в договоре



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Caja de Seguros Reunidos

**Когда:** 2022.10

**За что:** нарушение ст. 6(1) GDPR

**Как:** штраф €40,000, который был уменьшен до €24,000

**Причина:** компания незаконно изменила информацию, включенную в договор между ней и физическим лицом, что привело к несанкционированной обработке персональных данных последнего.

## Штраф за оставление посылки соседу субъекта данных без его предварительного согласия



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** United Parcel Service España Ltd

**Когда:** 2022.11

**За что:** нарушение ст. 5(1)(f), 32 GDPR

**Как:** штраф €70,000

**Причина:** Субъект данных подал жалобу, поскольку курьерская компания United Parcel Service (UPS) доставила адресованную ему посылку соседу без предварительного согласия.

UPS утверждал, что с Media Markt был заключен договор и что они действовали как поставщики услуг, следуя их инструкциям и действуя в соответствии с договором. Они также утверждали, что в пункте 10 договора указано, что посылки могут быть оставлены у соседей, если адресат не может быть найден; а в пункте 11 указано, что именно Media Markt должен информировать своего клиента об обработке его данных.

Согласно позиции AEPD, договор между UPS и Media Markt не содержит признаков поручения обработки данных, т.е. UPS не может квалифицироваться как обработчик и ответственен за инцидент из-за фактического контроля над средствами обработки персональных данных.

## 896 Штраф за нарушения в длительности хранения учетных записей



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Discord Inc.

**Когда:** 2022.11

**За что:** нарушение ст.5(1)е, 13, 25(2), 32, 35 GDPR

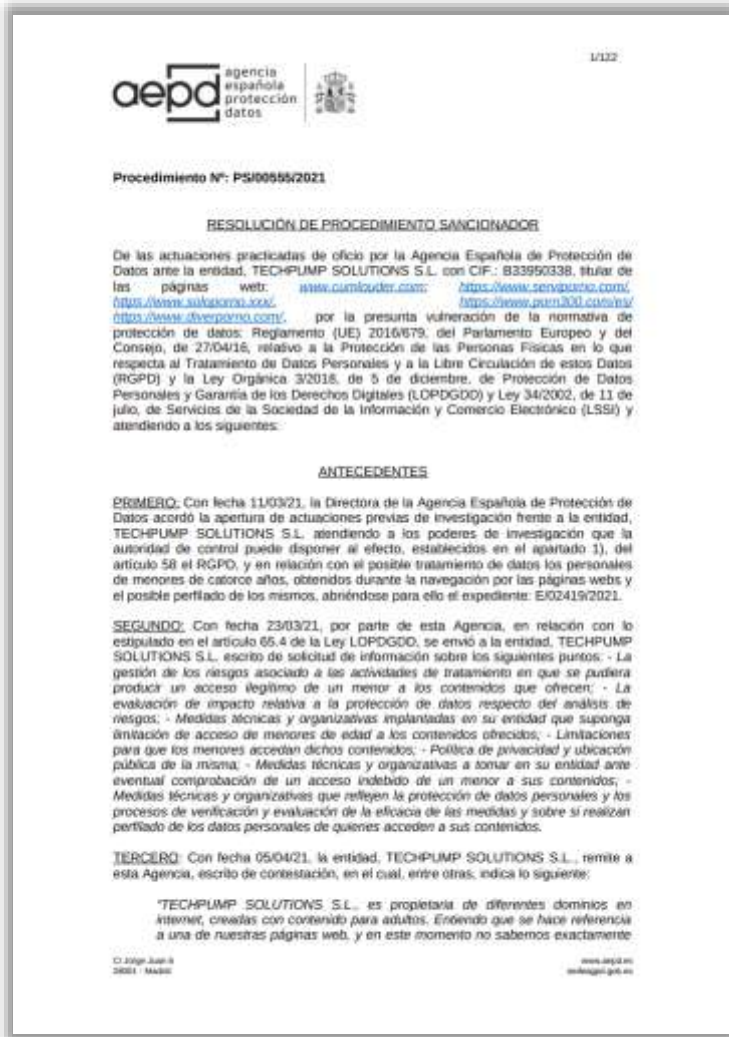
**Как:** штраф €800,000

**Причина:** в базе данных контролера хранились аккаунты почти 2,5 миллионов французов, которые не использовались более трех лет. Теперь платформа обязуется удалять учетные записи пользователей после двух лет бездействия.

Discord принимает слишком простые пароли (из шести символов). Теперь платформа требует более длинные и сложные пароли.

CNIL также предупредила, что после закрытия окна Discord пользователь не выходит из голосового чата автоматически. Чтобы решить эту проблему, платформа установила всплывающее окно, которое предупреждает людей о том, что приложение может работать в фоновом режиме после закрытия окна.





**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Techpump Solutions S.L.

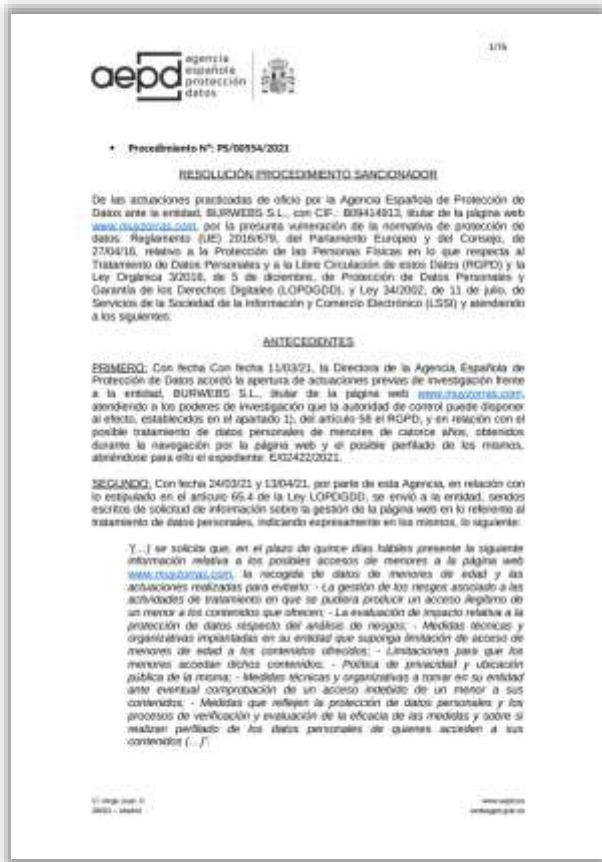
**Когда:** 2022.11

**За что:** нарушение ст. 5(1)(a),(b),(e), 6(1), 8, 12(1),(2), 13, 22(2), 25, 30(1) GDPR

**Как:** штраф €525,000

**Причина:** Techpump управляет несколькими веб-сайтами с контентом для взрослых. Выявленные нарушения:

1. вопреки указанной информации в политике конфиденциальности, Techpump делилась данными пользователей с компаниями, входящими в одну группу;
2. не указан срок хранения персональных данных пользователей и хранила их неопределенное время, пока пользователи не запросили отзыв своего согласия;
3. обработка персональные данные пользователей без предварительного получения их согласия;
4. отсутствие достаточных средств родительского контроля для предотвращения доступа несовершеннолетних в возрасте до 14 лет к его контенту;
5. политика конфиденциальности была доступна только на английском, а не на испанском языке;
6. Techpump также требовал, чтобы лица, желающие воспользоваться своими правами субъекта данных, предоставляли данные своего удостоверения личности для подтверждения своей личности;
7. Techpump также собирал различные данные, такие как IP-адреса и данные WIFI, не определив цели их обработки.



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Burwebs S.L. (владелец различных Интернет-ресурсов, каждый из которых содержит материалы для взрослых)

**Когда:** 2022.11

**За что:** нарушение ст. 5(1)(a), 5(1)(b), 5(1)(e), 8, 12(2), 13, 25, 30(1) GDPR и ст.22(2) Закона № 34/2002 от 11.07.2022 об услугах информационного общества и электронной торговле ("LSSI")

**Как:** штраф €75,000

**Причина:** 1. Обработка данных не соответствует политике конфиденциальности Burwebs (ст. 5(1)(a) GDPR).

2. Персональные данные пользователей Интернет-ресурсов обрабатывались бессрочно (ст. 5(1)(b) и 5(1)(e) GDPR).

3. Обработка данных несовершеннолетних пользователей, зарегистрированных в качестве пользователей без согласия их законных представителей (ст. 8 GDPR).

4. Процедура создания учетной записи не предусматривает проверку личности пользователя с помощью другой информации или мер, отличных от тех подтверждающих документов (ст. 12(2) GDPR).

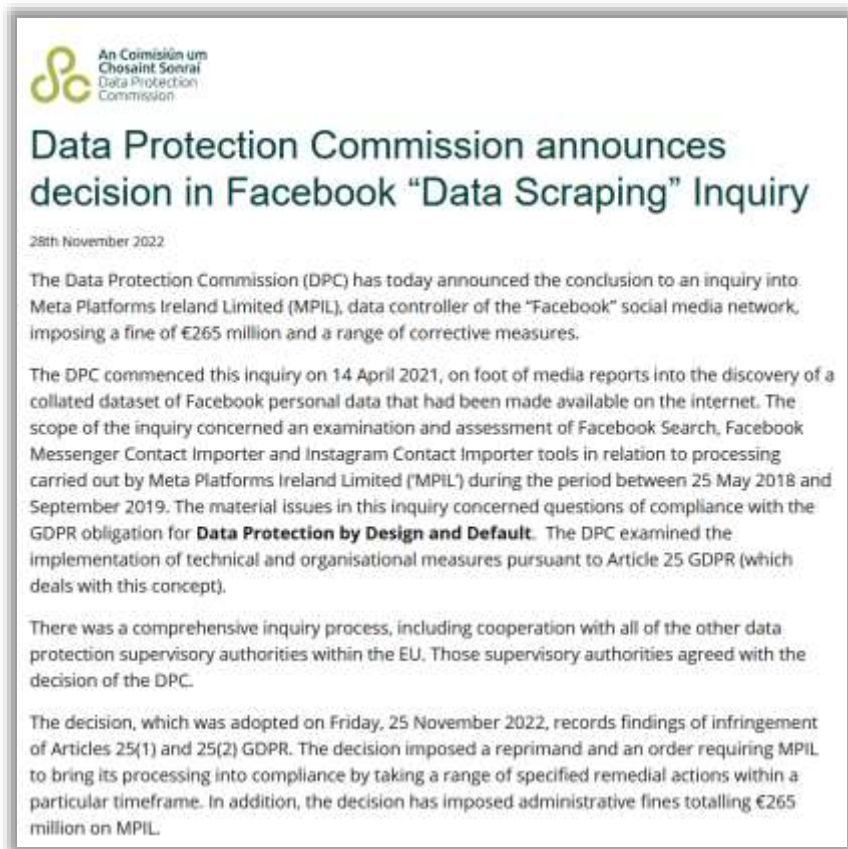
5. Политика конфиденциальности не информировала пользователей о возможности отзыва согласия в любое время и о периоде обработки персональных данных (ст. 13 GDPR).

6. Отсутствие подхода Privacy by Design и в неспособность оценить необходимость обработки данных (ст. 25 GDPR).

7. RoPA не описывал процесс обработки данных незарегистрированных пользователей (ст. 30(1) GDPR).

8. Пользователям не была предоставлена информация об обработке cookies, а также применялись т.н. «стены cookie» (ст. 22(2) LSSI).

## 899 Штраф на Facebook за возможность "скремблирования данных"



**Кто:** Data Protection Commission (Ирландия)

**Кого:** Meta Platforms Ireland Limited

**Когда:** 2022.11

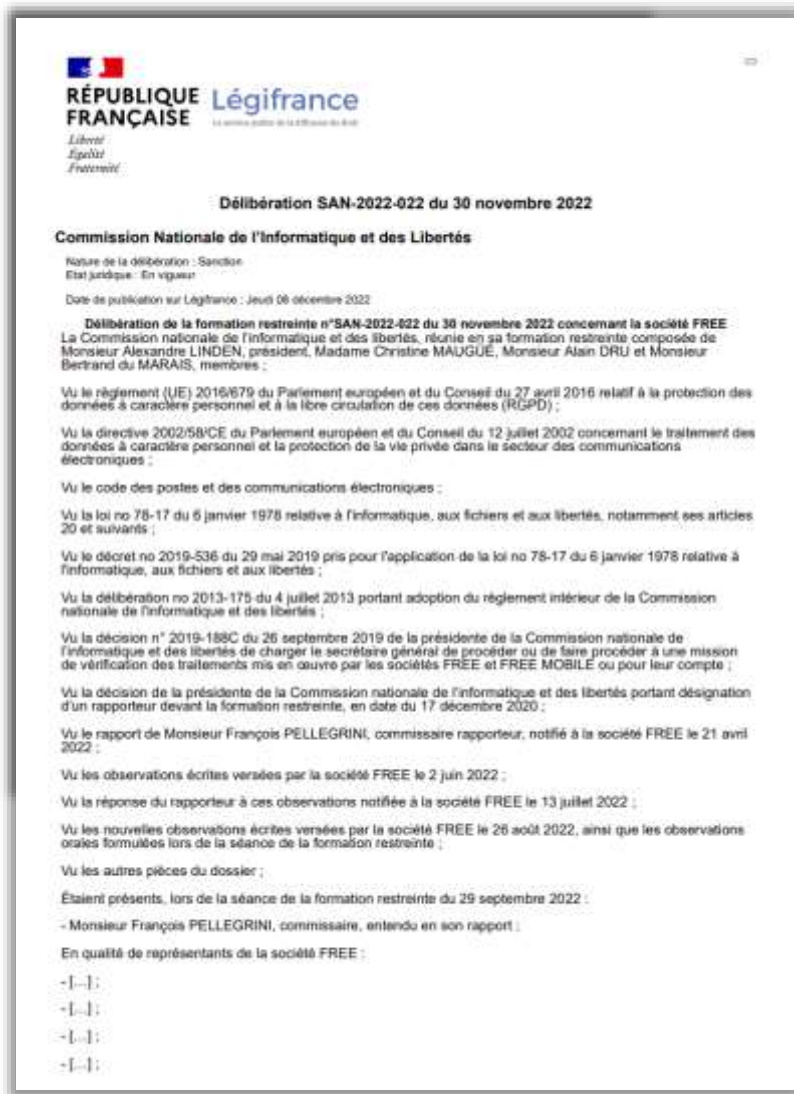
**За что:** нарушение ст. 25(1), 25(2) GDPR

**Как:** штраф €265,000,000 и несколько предписаний

**Причина:** штраф стал результатом расследования, начатого в прошлом году, в ходе которого было обнаружено, что в период с мая 2018 года по сентябрь 2019 года из Facebook был незаконно получен набор персональных данных, которые стали доступны в Интернете.

Meta заявила, что она добросовестно сотрудничала с расследованием Ирландского комиссара по защите данных (DPC) и внесла изменения в свои системы за указанное время, в том числе устранила возможность скремблирования данных своих пользователей с помощью проверки телефонных номеров.

## Штраф за несоблюдение прав субъектов данных и необеспечение безопасности пользовательских данных



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Free Mobile SAS

**Когда:** 2022.11

**За что:** нарушение ст. 12(3), 15, 17(1)(a), 32, 33 GDPR

**Как:** штраф €300,000

**Причина:** в ходе расследования CNIL установил, что компания Free не обеспечила в достаточной степени соблюдение прав субъектов данных, в частности, права на доступ и права на удаление, а также не приняла надлежащих мер по обеспечению безопасности данных, поскольку Free использовала недостаточно надежные пароли и допускала хранение и передачу простых текстовых паролей.

Среди прочего, CNIL отклонил утверждение о том, что источники персональных данных контролера считались "коммерческой тайной", и постановил, что контролер не смог адекватно ответить на запросы о доступе и уничтожении данных.

## 901 Штраф за нарушения при получении согласия на обработку cookies



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Electricité de France ("EDF")

**Когда:** 2022.11

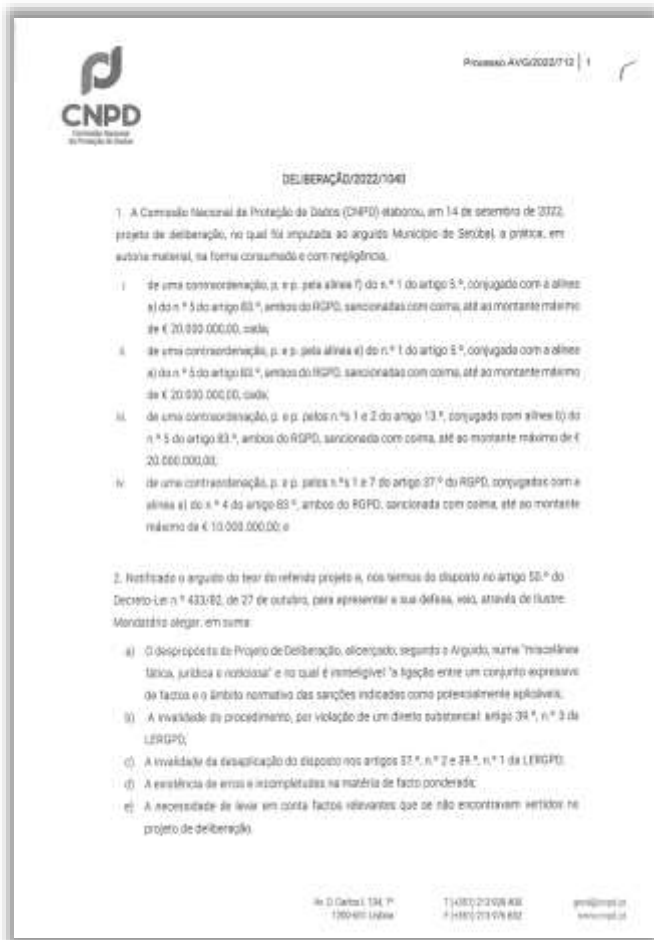
**За что:** нарушение ст. 7(1), 12, 13, 14, 15, 21, 32 GDPR и ст. L.34-5 Кодекса почтовой и электронной связи

**Как:** штраф €600,000

**Причина:** EDF не получила предварительного действительного согласия от физических лиц на проведение коммерческой поисковой кампании (поиск новых клиентов). На сайте EDF не было указано правовое основание, соответствующее каждому использованию данных, точная продолжительность хранения, а также точное место, откуда поступили данные, среди прочего. Также контролер не ответил на некоторые жалобы в течение одного месяца, предоставил неточную информацию об источнике собранных данных и не принял во внимание возражения, полученные в связи с коммерческим поиском.

EDF также нарушила обязательство по обеспечению безопасности персональных данных, поскольку пароли для доступа к клиентской зоне портала prime energy для более чем 25,000 счетов хранились в незащищенном виде до июля 2022 года, а пароли были только хэшированы, без соли (добавления случайных символов перед хэшем, чтобы избежать подбора пароля путем сравнения хэшей), что подвергало их риску.

## 902 Штраф за незаконную обработку персональных данных беженцев



**Кто:** Comissão Nacional de Protecção de Dados (Португалия)

**Кого:** муниципалитет Сетубала

**Когда:** 2022.11

**За что:** нарушение ст. 5(1)(f), 5(1)(e), 13(1), 13(2), 37(1), 37(7) GDPR

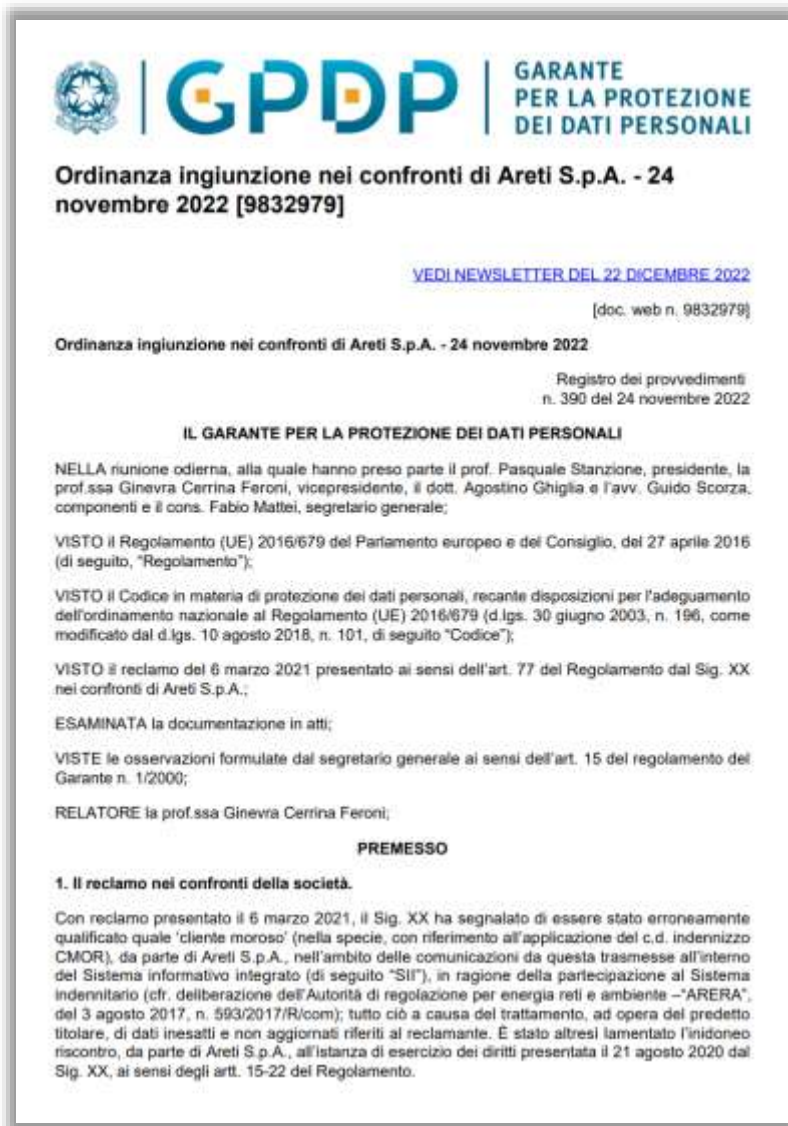
**Как:** штраф €170,000

**Причина:** решение касается действий муниципалитета по сбору персональных данных украинских беженцев. Муниципалитет попросил беженцев заполнить анкеты, содержащие обширную личную информацию о них, включая имя, адрес, дату рождения, семейное положение и информацию о документах, удостоверяющих личность.

CNPd установил, что муниципалитет не провел оценку воздействия на защиту данных ("DPIA"), несмотря на то, что беженцы считаются уязвимыми лицами в соответствии с Руководством по оценке воздействия на защиту данных Европейского надзора по защите данных ("EDPS"). Для информации, собранной муниципалитетом, не были определены сроки хранения, а также не были приняты достаточные технические и организационные меры.

Во время сбора данных субъектам данных не была предоставлена информация о контролере, целях обработки, получателях или категориях получателей персональных данных, правах субъектов данных и праве подать жалобу в надзорный орган. Муниципалитет не назначил DPO.

## 903 Штраф за обработку устаревших и неточных данных



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Areti S.p.A.

**Когда:** 2022.11

**За что:** нарушение ст. 5(1)(d), 5(1)(e), 5(2), 12(3), 15, 24 GDPR

**Как:** штраф €1,000,000

**Причина:** клиент компании был ошибочно отнесен к категории клиентов, имеющих задолженность, компанией Areti, поставщиком электроэнергии, из-за обработки неточных и устаревших данных. Как следствие, субъект данных не мог перейти к другому поставщику энергии. Кроме того, субъект получил неадекватный ответ компании Areti на его запрос о реализации прав как субъекта данных.

Невозможность смены поставщика для заявителя стала результатом обработки неточных и устаревших данных из-за несогласованности внутренних систем Areti, что привело к неправильному сообщению о текущей задолженности в Интегрированную информационную систему ("IIS"), базу данных, к которой обращаются поставщики перед подписанием нового контракта с пользователем. Из-за различных технических ошибок Areti ошибочно отнесла более 47,000 потенциальных клиентов к категории "имеющих задолженность", что привело к обработке неточных и устаревших данных.

## 904 Штраф на владельца Clubhouse за многочисленные нарушения GDPR



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Alpha Exploration Co. Inc. (владелец мобильного приложения Clubhouse)

**Когда:** 2022.12

**За что:** нарушение ст. 5(1)(a), 5(1)(e), 5(1)(f), 6, 7, 12(1), 13(1)(a), 14, 27(4), 28, 32, 35 GDPR

**Как:** штраф €2,000,000

**Причина:** в ходе расследования итальянский орган по защите данных («Garante») выявил многочисленные нарушения, например, отсутствие прозрачности в отношении использования данных пользователей и их контактов в чате. Кроме того, пользователи социальной сети могли хранить и обмениваться аудиосообщениями других пользователей без их согласия. Информация об учетной записи передавалась неавторизованным третьим лицам без надлежащего юридического основания. Кроме того, компания не определила сроки хранения персональных данных. Также компания не предоставила пользователям достаточной информации о многочисленных аспектах обработки их персональных данных и не внедрила достаточные технические и организационные меры для защиты персональных данных. Наконец, компания не провела оценку воздействия на защиту данных.



## 905 Штраф за нарушения при получении согласия на обработку cookies



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Microsoft Ireland Operations Limited

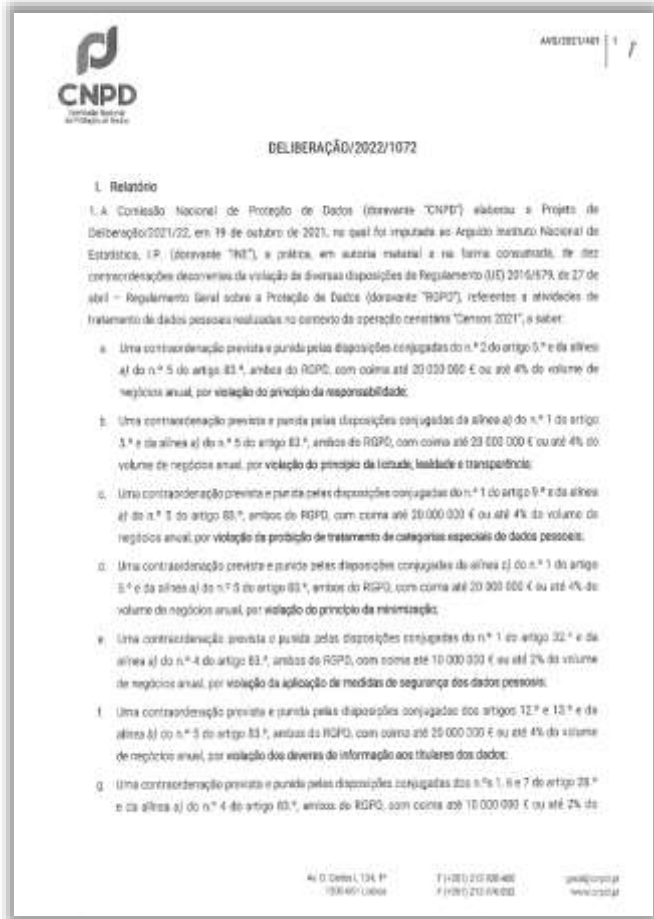
**Когда:** 2022.12

**За что:** нарушение ст.82 Закона №78-17 от 06.01.1978 "Об обработке данных, файлах данных и свободах личности"

**Как:** штраф €60,000,000

**Причина:** при посещении пользователями сайта [bing.com](https://www.bing.com) на пользовательские устройства без их согласия помещались файлы cookie, которые использовались с несколькими целями, включая противодействие рекламному мошенничеству, а когда пользователи продолжали использовать поисковую систему Bing, на их устройство помещался файл cookie с рекламной целью, опять же без получения согласия пользователей. CNIL указала, что, хотя поисковая система предлагала веб-баннер с кнопкой для немедленного принятия файлов cookie, она не предложила эквивалентного решения (кнопку для отказа или другое), чтобы пользователь мог так же легко отказаться от них.

В связи с вышеизложенным, CNIL приняла решение о наложении штрафа в вышеуказанном размере на компанию Microsoft, а также о вынесении судебного запрета, предписывающего Microsoft в течение трех месяцев изменить методы сбора согласия пользователей, находящихся во Франции, на использование файлов cookie, предложив им такое же простое средство отказа, как и механизм, предусмотренный для их принятия, а также предусматривающего наложение дополнительных штрафов в размере €60,000 за каждый день несоблюдения требований по истечении этого периода.



**Кто:** Comissão Nacional de Protecção de Dados (Португалия)

**Кого:** Национальный институт статистики

**Когда:** 2022.12

**За что:** нарушение ст. 9(1), 12, 13, 28(1), 28(6), 28(7), 35(1), 35(2), 35(3)(b), 44, 46(2) GDPR

**Как:** штраф €4,300,000

**Причина:** Национальный институт, обрабатывая специальные данные, касающиеся здоровья и религии, не предоставил четкой и полной информации о необязательном характере их предоставления гражданами и не объяснил в достаточной мере, что некоторые из вопросов являются необязательными, тем самым не дав гражданам возможности сформировать свою волю, что является необходимым для предположений о законности обработки этих специальных категорий данных.

Кроме того, контролер заключил договор с компанией Cloudflare, Inc., базирующейся в США, на обработку данных в любом из 200 серверов Cloudflare, при этом обе компании предполагали, что данные могут обрабатываться за пределами ЕЭЗ. Хотя договор также включал в себя SCC для передачи персональных данных в США, но не предусматривал никаких дополнительных мер безопасности, как того требует решение CJEU по делу Schrems II. Национальный институт не проводил никакой оценки воздействия на защиту данных ("DPIA"), связанной с обработкой.

## 907 Штраф за ненадлежащее согласие в отношении рекламы



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Apple Distribution International Ltd.

**Когда:** 2022.12

**За что:** нарушение ст.82 Закона №78-17 от 06.01.1978 "Об обработке данных, файлах данных и свободах личности"

**Как:** штраф €8,000,000

**Причина:** настройки персонализированной рекламы на устройствах Apple активированы по умолчанию, и это не позволяют пользователям дать действительное согласие на целевую рекламу.

CNIL установила, что идентификаторы Apple, имеющие несколько целевых назначений, в том числе персонализированной рекламы, по умолчанию автоматически обрабатываются на устройствах Apple. Такие идентификаторы не являются строго необходимыми для предоставления услуги по использованию App Store и не должны обрабатываться Apple без предварительного согласия пользователей.

CNIL подчеркнула, что для успешной деактивации таких настроек по умолчанию пользователи должны были выполнить несколько действий, поскольку такая возможность не была интегрирована в процесс инициализации устройств Apple. Такой процесс деактивации не соответствует требованиям по получению предварительного согласия пользователей на обработку с рекламными целями.



**Кто:** Data Protection Commission (Ирландия)

**Кого:** Meta Platforms Ireland Limited (владеет социальными сетями Facebook и Instagram, мессенджером WhatsApp)

**Когда:** 2022.12

**За что:** нарушение ст. 5(1)(a), 6, 12, 13(1)(c) GDPR

**Как:** штрафы €210,000,000 (за нарушения Facebook) и €180,000,000 (за нарушения Instagram), предписание устранить нарушения GDPR за 3 месяца

**Причина:** пользователи Facebook и Instagram не имели достаточной ясности в отношении того, какие операции по обработке выполнялись с их персональными данными, с какой целью (целями) и на каком правовом основании. Кроме того, Meta не имела права полагаться на правовую основу в виде "договора" (пользовательского соглашения) в связи с применением поведенческой рекламы в рамках своих сервисов Facebook и Instagram.

<https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland>

[https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-42022-dispute-submitted\\_en](https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-42022-dispute-submitted_en)

<https://noyb.eu/en/meta-advertising-ban-decision-published>

## 909 Штраф за некорректное правовое основание для обработки данных

**Кто:** Data Protection Commission (Ирландия)

**Кого:** WhatsApp Ireland Ltd.

**Когда:** 2023.01

**За что:** нарушение ст. 6(1), 12, 13(1)(c) GDPR

**Как:** штрафы €5,500,000 и предписание устранить нарушения GDPR за 6 месяцев

**Причина:** в новых условиях обслуживания WhatsApp проинформировал своих пользователей о необходимости нажать кнопку "Согласиться и продолжить", чтобы выразить свое согласие с новыми условиями обслуживания. Это требовалось для дальнейшего доступа к услугам. WhatsApp предполагал, что принятие обновленных условий использования представляет собой договор между WhatsApp и пользователем, поскольку обработка данных будет необходима для предоставления и улучшения услуг. По мнению WhatsApp, обработка данных была законной в соответствии со ст. 6(1)(b) GDPR.

Однако WhatsApp фактически пытается полагаться на согласие как на правовую основу для обработки данных пользователей. Ставя доступ к своим услугам в зависимость от согласия пользователей с обновленными условиями предоставления услуг, WhatsApp вынуждал пользователей давать согласие на обработку своих персональных данных.

DPC установил, что WhatsApp не полагался на согласие пользователей в качестве правовой основы и не рассматривал "принудительное согласие" в данном случае. Он также не исключил возможность того, что WhatsApp опирался на договорную правовую основу. Однако DPC пришел к выводу, что WhatsApp нарушил свои обязательства по прозрачности в соответствии с GDPR, не объяснив пользователям, с какой целью и на каком законном основании будут обрабатываться их персональные данные. По итогам расследования DPC представил проект решения в соответствии со ст.60 GDPR другим заинтересованным европейским надзорным органам.

В ответ DPC получил возражения от различных надзорных органов. Поскольку по спорным пунктам не удалось достичь соглашения, DPC инициировал процедуру разрешения спора в соответствии со ст.65 GDPR. В своем решении EDPB подтвердил нарушение компанией WhatsApp обязательств по обеспечению прозрачности. Однако EDPB занял иную позицию, чем DPC, по вопросу правовой основы и постановил, что WhatsApp не имел права полагаться на договорную правовую основу. Поэтому EDPB постановил, что WhatsApp нарушил ст. 6 (1) GDPR. DPC согласился с этим в своем окончательном решении и наложил штраф, а также обязал WhatsApp привести обработку данных в соответствие с требованиями GDPR.

## Штраф за незаконную пересылку входящей электронной почты бывшего работника

**Personvernemnda**

Personvernemndas vedtak 13. desember 2022 (Mari Bø Haugstad, Bjørnar Borvik, Hans Marius Graasvold, Heidi Talsethagen, Hans Marius Tessem, Morten Goodwin, Malin Tønseth)

**PVN-2022-14 Overvåking av arbeidstakers e-postkasse uten rettslig grunnlag - overtredelsesgebyr**

Datatilsynets referanse: 23/02368-0

Saken gjelder klage fra X AS over Datatilsynets utstilling av overtredelsesgebyr på 100 000 kroner for å ha overvåket arbeidstakers e-postkasse uten rettslig grunnlag, jf. personvernforordningen artikkel 6 nr. 1 bokstav f, for manglende vurdering av protester, jf. artikkel 21 og for manglende informasjon, jf. artikkel 13.

X AS har også klaget over Datatilsynets pålegg om å utarbeide interne rutiner for innsyn i ansattes og tidligere ansattes e-postkasser og annet elektronisk lagret materiale, jf. artikkel 24.

**Sakens bakgrunn**

X AS sendte 3. oktober 2019 en avklarende melding til Datatilsynet om at selskapet hadde foretatt innsyn i tidligere arbeidstakers e-postkasser uten å ha rettslig grunnlag for dette. Avklarende meldingen ble sendt etter at tidligere arbeidstaker hadde gjort selskapet oppmerksom på at innsyn og automatisk videreledning av e-post var ulovlig.

Datatilsynet mottok brevets 10. oktober 2019 en klage fra A om at hennes tidligere arbeidsgiver, X AS, hadde foretatt ulovlig innsyn i og automatisk videreledning av hennes e-post etter at hun sluttet i selskapet.

Datatilsynet ble 26. november 2020 om arbeidsgivers ledelse, som etter utsett avforret, ble gitt 14. januar 2021.

Datatilsynet varslert arbeidsgiver 1. juli 2021 om at selskapet ville treffe alle vedtak:

1. Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i pålegges X AS, org. nr. [redacted], å betale et overtredelsesgebyr til statkassen på kr 100 000 for automatisk videreledning av klagers e-postkasser, jf. personvernforordningen artikkel 6 nr. 1 bokstav f, for manglende vurdering av protester, jf. artikkel 21, og for manglende informasjon, jf. artikkel 13.
2. X AS pålegges å utarbeide interne rutiner og rutiner for innsyn i ansattes og tidligere ansattes e-postkasser og annet elektronisk lagret materiale, jf. personvernforordningen artikkel 24.

Arbeidsgiver ga sine merknader til varsellet 13. september 2021 og la ved selskapets sjekkliste for ivaretagelse av personvern når ansatte slutter, samt utkast på selskapsnettskjema for innsyn/videreledning av e-post etter avsluttet arbeidsforhold.

Datatilsynet traff 15. mars 2022 vedtak om pålegg og overtredelsesgebyr i slikt med utsettelse varsel.

Arbeidsgiver klaget rettslig på Datatilsynets vedtak 28. mars 2022. Klagen gjelder overtredelsesgebyrets størrelse og pålegget om å utarbeide interne rutiner for innsyn i ansattes e-postkasser.

Datatilsynet vurderte klagen, men fant ikke grunn til å endre sitt vedtak. Datatilsynet overvåket saken til Personvernemnda 24. juni 2022. Arbeidsgiver ble orientert om saken i brev fra emnda 25. juni 2022, og fikk anledning til å komme med kommentarer. Det er ikke innlagt kommentarer.

Saken ble behandlet i rettsutvalget møte 13. desember 2022. Personvernemnda hadde følgende sammensetning: Malin Tønseth (leder), Bjørnar Borvik (medleder), Hans Marius Graasvold, Heidi Talsethagen, Hans Marius Tessem, Morten Goodwin og Malin Tønseth. Sekretæransvar ligger på Morten Goodwin og også til stede.

**Kto:** Datatilsynet (Norge) и норвежский совет по защите частной жизни ("Personvernemnda") – после подачи апелляции на решение Datatilsynet

**Kogo:** неназванная компания

**Kогда:** 2022.12

**За что:** нарушение ст. 6(1)(f), 13, 24 GDPR и раздела 2(2) Регламента 1108/2018 о доступе работодателя к электронной почте и другим материалам, хранящимся в электронном виде ("Регламент мониторинга электронной почты")

**Как:** штраф €9,600

**Причина:** бывший работник пожаловался на то, что компания незаконно получала доступ к его электронной почте и автоматически пересылала ее после его увольнения. В частности, были выявлены следующие факты:

- осуществлялась автоматическая пересылка компанией содержания электронных писем бывшего работника;
- компания не провела LIA в отношении пересылки писем после возражения работника;
- компания не проинформировала работника о пересылке его электронной почты.

## Штраф за раскрытие компанией информации о привлечении бывшего работника к уголовной ответственности



**DATATILSYNET**

Politianmeldelse

### Privat virksomhed indstillet til bøde

Dato: 02-12-2022

Algerelse · Private virksomheder · Politianmeldelse · Klage · Strafbare forhold

Datatilsynet har politianmeldt en virksomhed og indstillet til bøde på 150.000 kr. for at have videregivet oplysninger om strafbare forhold uden hjemmel.



Datatilsynet har politianmeldt en virksomhed for uberettiget at have videregivet oplysninger om strafbare forhold om en tidligere medarbejder til en række af virksomhedens kunder. Datatilsynet har indstillet til en bøde på 150.000 kr.

Datatilsynet blev tidligere i år kontaktet af den tidligere medarbejder, som klagede over, at vedkommendes tidligere arbejdsgiver uberettiget havde videregivet oplysninger om strafbare forhold begået af medarbejderen til en række af virksomhedens kunder.

**Кто:** Datatilsynet (Дания)

**Кого:** неназванная компания

**Когда:** 2022.12

**За что:** нарушение ст. 5, 6 GDPR

**Как:** штраф €20,150

**Причина:** компания отправляла клиентам по электронной почте конкретную информацию с подробным описанием уголовных преступлений, совершенных бывшим работником в связи с его трудовой деятельностью.

Информации о привлечении к уголовной ответственности может быть раскрыта только при наличии разрешения в соответствии с п.4 ст.8 Закона №502 от 23.05.2018 о дополнительных положениях к Положению о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных. Например, раскрытие возможно для цели удовлетворения частных интересов, которые явно превышают соображения интересов секретности.

Компания имела законный интерес в передаче информации об увольнении бывшего работника своим клиентам и в информировании клиентов о том, что работник не может заключать договоры от имени компании, но более подробное описание обвинений против бывшего работника не было необходимым для достижения такой цели.

## 912 Штраф за мониторинг электронной корреспонденции работников



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Регион Лацио

**Когда:** 2022.12

**За что:** нарушение ст. 5(1)(a), 5(1)(e), 5(2), 6, 12, 13, 25, 35, 88(1) GDPR

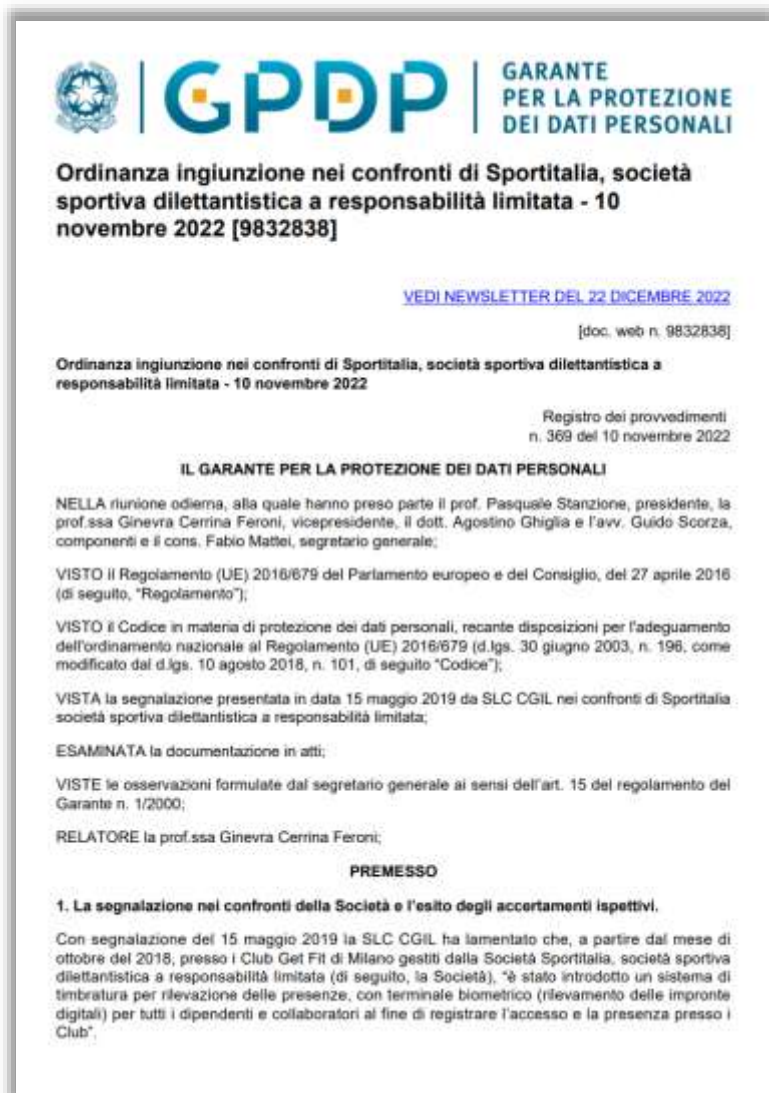
**Как:** штраф €100,000

**Причина:** Профсоюз подал жалобу в DPA, утверждая, что региональные власти мониторили электронные почтовые ящики и электронную корреспонденцию (метаданные сообщений) работников собственного юридического отдела области. Мониторинг был инициирован по подозрению в возможном раскрытии информации, охраняемой служебной тайной, третьим лицам.

Данные мониторинга хранились и анализировались в течение 180 дней, и включали не только информацию, связанную с работой, но и персональные данные субъектов данных, касающиеся их частной жизни.



## 913 Штраф за неправомерную обработку биометрических данных работников



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Sportitalia società sportiva dilettantistica a responsabilità limitata

**Когда:** 2022.12

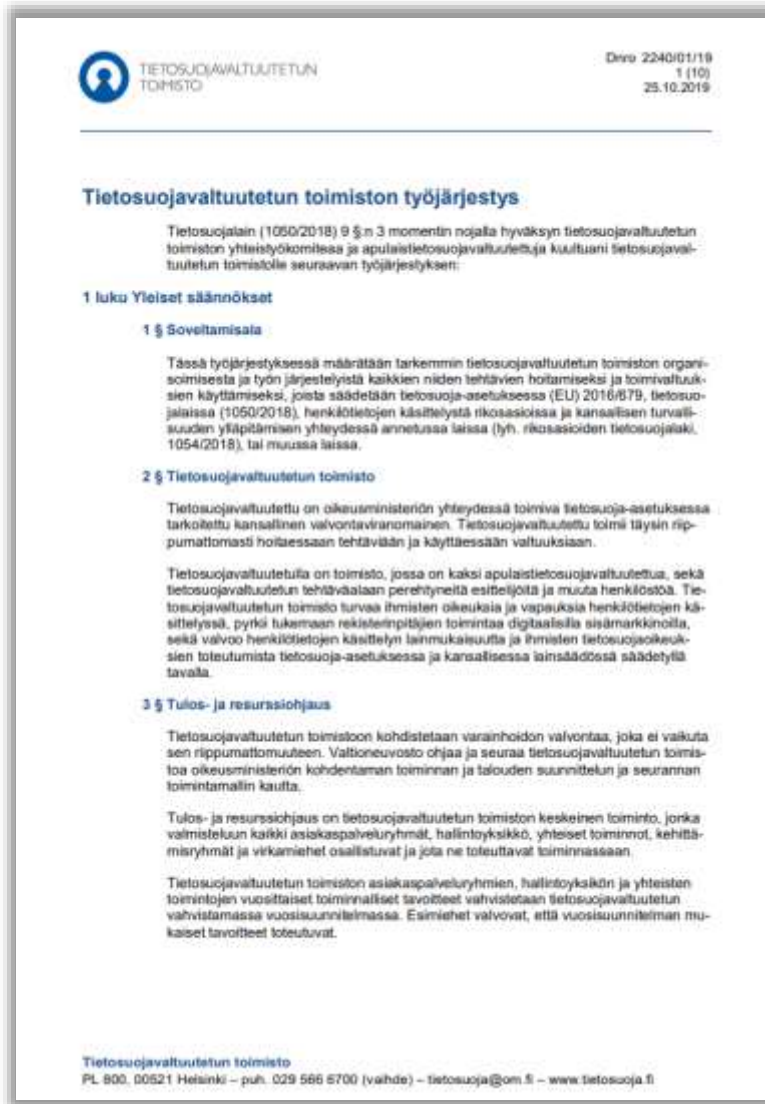
**За что:** нарушение ст. 5(1)(a), 9, 13, 30(1)(c) GDPR

**Как:** штраф €20,000

**Причина:** Sportitalia обрабатывала персональные данные своих работников посредством активации биометрической системы, предназначенной для определения присутствия на рабочем месте, основанной на сканировании отпечатков пальцев и их связи с кодом, присвоенным работнику, с целью облегчить работникам регистрацию времени входа и выхода и внедрить более упорядоченную и быструю систему по сравнению с ранее использовавшейся, основанной на сканировании пропусков.

Garante установил, что обработка биометрических данных была произведена в отсутствие адекватной правовой основы, учитывая, что сбор согласия субъектов данных в контексте трудовых отношений не соответствует GDPR. Информация, которую работодатель предоставил работникам в отношении обработки их биометрических данных, была недостаточной для представления характеристик обработки, которая будет осуществляться с помощью конкретных биометрических устройств

## 914 Штраф за непредоставление бывшему работнику доступа к его данным



**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

**Кого:** Viking Line Oy Abp


**Когда:** 2022.12

**За что:** нарушение ст. 5(1)(a), 5(1)(d), 12(3), 13, 15, 25(1) GDPR

**Как:** штраф €230,000

**Причина:** бывший работник компании Viking Line не получил все свои персональные данные, хранящиеся в компании, несмотря на то, что подал запрос на доступ. Кроме того, компания хранила данные о его здоровье в течение 20 лет и что некоторые хранившиеся сведения о диагнозе были неточными. Viking Line должна была хранить данные о состоянии здоровья работников отдельно от других персональных данных, а данные о здоровье должны были быть удалены сразу после того, как необходимость в их хранении отпала.

## 915 Штраф за непредоставление клиентам доступа к их данным

 TETOSUOJAVALTUUTETUN TOIMISTO 1 (28)

Dno 6633/182/2018  
6707/154/2018  
7885/152/2020  
13.12.2022

### APULAISTIETOSUOJAVALTUUTETUN PÄÄTÖS

**Asia** Rekisteröidyn oikeus saada tutustua tietoihin ja oikeus tietojen poistamiseen ym.

**Rekisterinpitäjä** Alektum Oy

**Hakijoiden vaatimukset perusteluineen**

1. Asian 6633/182/2018 hakija on kertonut, että Alektum Oy ei lainkaan ole vastannut hänen 26.8.2018 esittämäänsä pyyntöön saada tutustua tietoihin.
2. Asian 6707/154/2018 hakija on kertonut esittäneensä Alektum Oy:lle pyynnön saada tutustua tietoihin. Vastauksena hakijan pyyntöön hakijalle oli hakijan kertoman mukaan toimitettu vain otakkotasoista listaa niistä tiedoista, josta rekisterinpitäjä hänen osaltaan tuolloin käsiteli. Hakijalle ei ollut hakijan kertoman mukaan toimitettu hänen omia tietojaan. Hakija oli lisäksi pyytänyt, että hänen tietonsa poistettaisiin.
3. Asian 7885/152/2020 hakija on kertonut, että Alektum Oy ei lainkaan ole vastannut hänen 25.6.2020 esittämäänsä pyyntöön saada tutustua tietoihin.

**Asian selvittämisestä**

4. Tietosuojavaltuutetun toimistossa on ajalla 27.9.2018–1.10.2020 saatettu viereille useampia Alektum Oy:n suorittamaan henkilötietojen käsittelyyn liittyviä asioita, joissa on ollut kysymys rekisteröidyn oikeudesta saada tutustua tietoihin (oikeus tunnetaan myös nimellä tarkastusoikeus) ja oikeudesta tietojen poistamiseen. Hakijat ovat kertoneet, että Alektum Oy ei ole vastannut heidän esittämäänsä pyyntöihin, antanut pyydettyjä tietoja tai toteuttanut oikeutta tietojen poistamiseen.
5. Rekisterinpitäjältä on pyydetty selvitystä kysymyksessä olevista asioista. Ensimmäinen selvityspyyntö (6633/182/2018) on 30.3.2020 lähetetty rekisterinpitäjän omilla verkkosivulla (alektum.fi) tuolloin ilmoitettuun sähköpostiosoitteeseen [gdpr@annormen.fi](mailto:gdpr@annormen.fi).<sup>1</sup> Tähän sähköpostiosoitteeseen on niin ikään 8.4.2020 lähetetty toisen asian (6707/154/2018) ensimmäinen selvityspyyntö.<sup>2</sup> Koska rekisterinpitäjä ei vastannut 30.3.2020 lähetettyyn selvityspyntöön annetussa määräajassa, on selvityspyyntö lähetetty rekisterinpitäjälle uudelleen 20.4.2020 (osoitteisiin [gdpr@annormen.fi](mailto:gdpr@annormen.fi) ja [info@annormen.fi](mailto:info@annormen.fi)).<sup>3</sup> Samassa yhteydessä tietosuojavaltuutetun toimisto on tuolloin välittämistä poikkeuksellisista olosuhteista johtuen oma-aloitteisesti pidentänyt selvityspyntöön

<sup>1</sup> Ks. Liite 1, Sähköpostiviesti 30.3.2020.  
<sup>2</sup> Ks. Liite 2, Sähköpostiviesti 8.4.2020.  
<sup>3</sup> Ks. Liite 3, Muutatussähköpostiviesti 20.4.2020.

Tietosuojavaltuutetun toimisto  
PL 800, 00531 Helsinki – puh. (029 566 6700 (vaihde) – [tietosuoja@tom.fi](mailto:tietosuoja@tom.fi) – [www.tietosuoja.fi](http://www.tietosuoja.fi)

**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

**Кого:** Alektum Oy

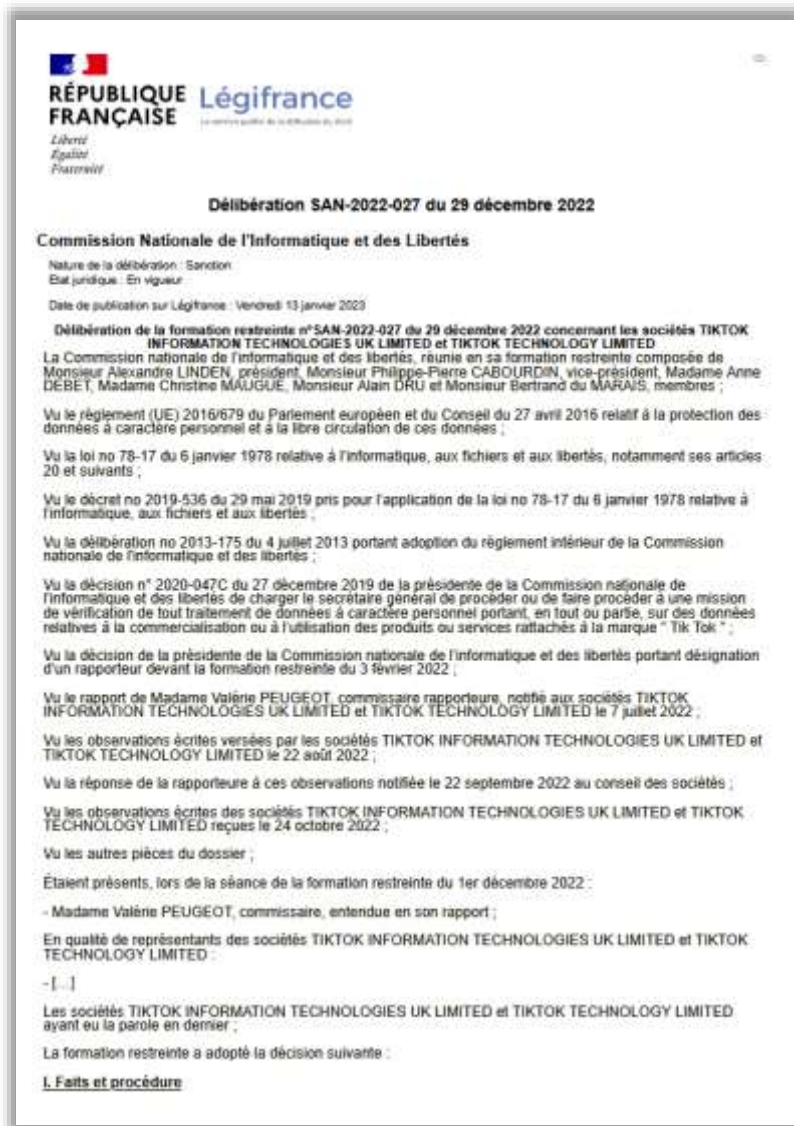
**Когда:** 2022.12

**За что:** нарушение ст. 12(3), 15(1), 15(3) GDPR

**Как:** штраф €750,000

**Причина:** трое заявителей утверждали, что компания Alektum не ответила на их запросы о доступе к их персональным данным. В практике обработки персональных данных компанией Alektum были серьезные недостатки. В частности, Alektum регулярно не отвечал на запросы, касающиеся прав субъекта данных на защиту информации. Кроме того, омбудсмен пояснил, что, несмотря на аргумент компании Alektum о том, что она больше не обрабатывает персональные данные субъектов данных, Alektum должна была ответить на запросы и упомянуть, что она больше не обрабатывает персональные данные заявителей.

## Штраф за использование непредоставление возможности отказаться от обработки файлов cookie



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** TikTok Information Technologies UK Limited и TikTok Technology Limited

**Когда:** 2022.12

**За что:** нарушение ст.82 Закона №78-17 от 06.01.1978 "Об обработке данных, файлах данных и свободах личности"


**Как:** штраф €2,500,000 на каждую из компаний

**Причина:** социальная сеть TikTok из-за усложнения процедуры отказа пользователей от обработки файлов cookie фактически вынуждает субъектов данных нажать кнопку «Принять все cookie».

В свою очередь TikTok ответил, что данные обвинения касаются только лишь старых действий, так как в минувшего году была введена возможность отказа от необязательных файлов cookie и предоставлена дополнительная информация о целях использования определенных файлов.

После запроса CNIL на упрощение процедуры отказа от файлов cookie ситуация в корне никак не изменилась, а потому регулятор принял решение о наложении штрафа.

# Штраф за использование идентификаторов мобильного приложения для профилирования и таргетирования

 **RÉPUBLIQUE FRANÇAISE** **Légifrance**  
Le service public de la diffusion du droit  
*Liberté  
Égalité  
Fraternité*

**Délibération SAN-2022-026 du 29 décembre 2022**

**Commission Nationale de l'Informatique et des Libertés**

Nature de la délibération : Sanction  
Etat juridique : En vigueur  
Date de publication sur Légifrance : Mardi 17 janvier 2023

**Délibération de la formation restreinte no SAN-2022-026 du 29 décembre 2022 concernant la société VOODOO**  
La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Monsieur Philippe-Pierre CABOURDIN, vice-président, Madame Anne DEBET, Madame Christine MAUGUÉ et Monsieur Alain DRU, membres ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2021-194C de la présidente de la CNIL du 29 juin 2021 de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société VOODOO ou pour son compte ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte du 20 juin 2022 ;

Vu le rapport de Monsieur Claude CASTELLUCCIA, commissaire rapporteur, notifié à la société VOODOO le 22 juillet 2022 ;

Vu les observations écrites versées par la société VOODOO le 26 septembre 2022 ;

Vu la réponse du rapporteur à ces observations notifiée le 21 octobre 2022 au conseil de la société ;

Vu les observations écrites de la société VOODOO reçues le 21 novembre 2022 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 8 décembre 2022 :

- Monsieur Claude CASTELLUCCIA, commissaire, entendu en son rapport ;

En qualité de représentants de la société VOODOO :

- [...]

La société VOODOO ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

**I. Faits et procédure**

1. Créée en 2013, la société VOODOO (ci-après "la société"), spécialisée dans l'édition de jeux pour téléphone, est une société par actions simplifiée dont le siège social est situé 17 rue Henry Monnier à Paris (75009). En septembre 2021, le groupe VOODOO, qui comporte une vingtaine de sociétés, employait [...] personnes en France, dont [...] au sein de la société VOODOO. La société détient plusieurs filiales au sein de plusieurs Etats membres de l'Union européenne dont l'activité exclusive est le développement de jeux mobiles qui sont ensuite publiés et exploités par la société VOODOO.

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** VOODOO SAS

**Когда:** 2023.01

**За что:** нарушение ст.82 Закона №78-17 от 06.01.1978 "Об обработке данных, файлах данных и свободах личности"

**Как:** штраф €3,000,000 + предписание в течение 3 месяцев устранить нарушение (доп. штраф €20,000 просрочки исполнения предписания)

**Причина:** в период с августа 2021 года по июль 2022 года было проведено несколько проверок сайта voodoo.io и различных мобильных приложений компании VOODOO (например, игра Helix Jump). Когда издатель размещает приложение в App Store, Apple Inc. предоставляет ему систему технической идентификации "IDentifier For Vendors" ("IDFV"), которая позволяет издателю отслеживать использование его приложений пользователями, что позволяет персонализировать рекламу. VOODOO использовала IDFV без явного и свободного согласия пользователей, которые не дали своего согласия на эту операцию через окно в приложении.

<https://www.cnil.fr/fr/jeux-mobiles-la-cnil-sanctionne-voodoo-hauteur-de-3-millions-deuros>

[https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046988935?init=true&page=1&query=SAN-2022-026&searchField=ALL&tab\\_selection=all](https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046988935?init=true&page=1&query=SAN-2022-026&searchField=ALL&tab_selection=all)

## Штраф за неадекватные меры безопасности данных, ставшие причиной уничтожению данных



**Кто:** Data Protection Commission (Ирландия)

**Кого:** Centric Health

**Когда:** 2023.01

**За что:** нарушение ст. 5(1)(f), 5(2), 32(1) GDPR

**Как:** штраф €460,000

**Причина:** DPC 05.12.2019 получил от Centric Health уведомление о нарушении защиты персональных данных, затронувшей данные пациентов, хранящиеся в системе управления пациентами Centric Health. Атака привела несанкционированному доступу, изменению и потере доступности персональных данных и данных специальной категории 70,000 субъектов данных. Данные 2,500 пациентов были удалены без возможности восстановления.

При обработке персональных данных в системе управления пациентами Centric Health не смогла обеспечить обработку персональных данных таким образом, чтобы обеспечить надлежащую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки, а также от случайной потери, уничтожения или повреждения.

## Штраф за неадекватные меры безопасности данных, ставшие причиной утечки данных



**Кто:** Data Protection Commission (Ирландия)

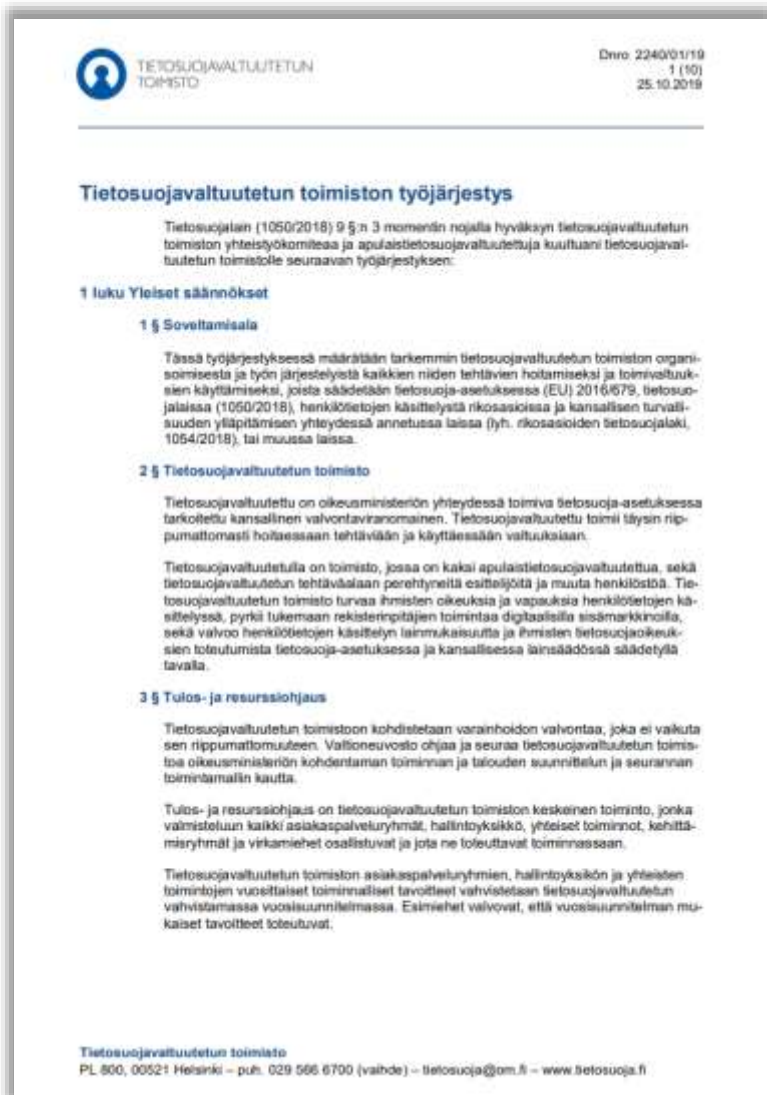
**Кого:** Bank of Ireland Group Plc ('BOI')

**Когда:** 2023.02

**За что:** нарушение ст. 5(1)(f), 32(1) GDPR

**Как:** штраф €750,000

**Причина:** DPC получил уведомление о нарушении защиты персональных данных от BOI в связи с 10 утечками данных в банковском приложении BOI365, которые касались лиц, получивших несанкционированный доступ к чужим счетам через приложение BOI365. BOI нарушила ст. 5(1) и 32(1) GDPR, поскольку технические и организационные меры, действовавшие на тот момент, были недостаточны для обеспечения безопасности персональных данных, обрабатываемых в приложении BOI365.



**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

**Кого:** Suomen Asiakastieto Oy

**Когда:** 2023.02

**За что:** нарушение ст.58(2) GDPR

**Как:** штраф €440,000

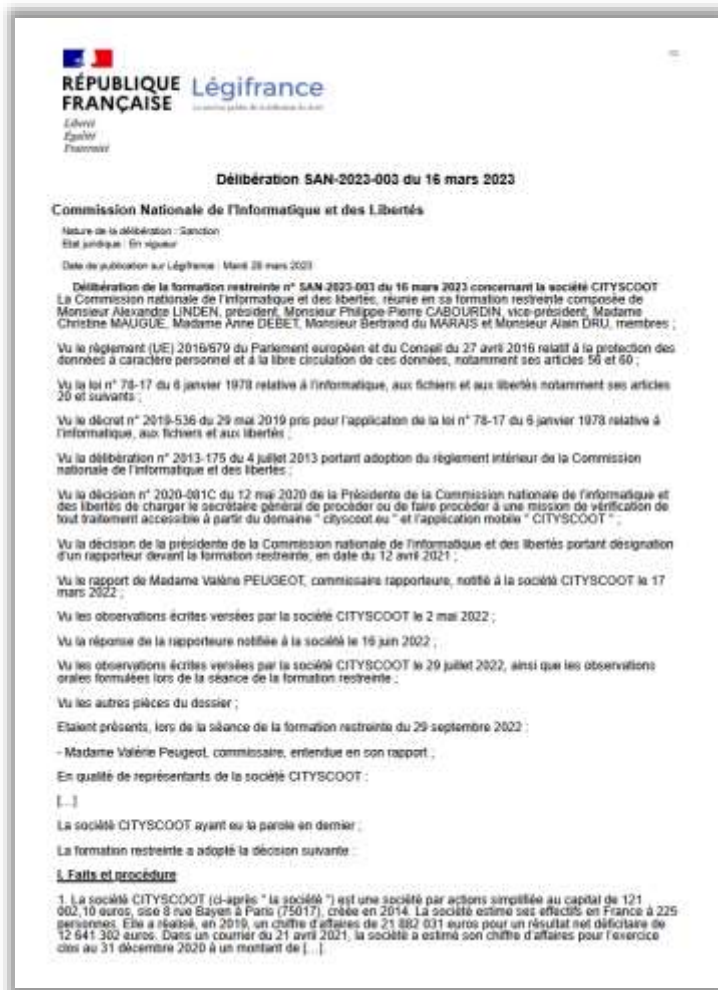
**Причина:** надзорный орган расследовал деятельность компании Suomen Asiakastieto по обработке информации о неисполнении обязательств по платежам, основанной на юридически обязательных судебных решениях, и что в то время он заявил, что информация, основанная на судебных решениях, вынесенных в ходе судебного процесса, не должна была регистрироваться как записи о неисполнении обязательств по платежам.

В ноябре 2021 года надзорный орган предписал Suomen Asiakastieto исправить свои операционные процедуры при регистрации информации о неисполнении платежей, основанной на судебных решениях, имеющих обязательную юридическую силу, и удалить все появившиеся неверные записи о неисполнении платежей.

Надзорный орган установил, что в практике Suomen Asiakastieto имеются недостатки в части своевременного выполнения предписания. Так, Suomen Asiakastieto предприняла действия несвоевременно, что привело к нарушению ст.58(2) GDPR.



## 921 Штраф за неправомерный сбор и обработку данных геолокации



**Кто:** Commission nationale de l'informatique et des libertés (Франция) в сотрудничестве с AEPD (Испания) и Garante (Италия)

**Кого:** Cityscoot SAS

**Когда:** 2023.03

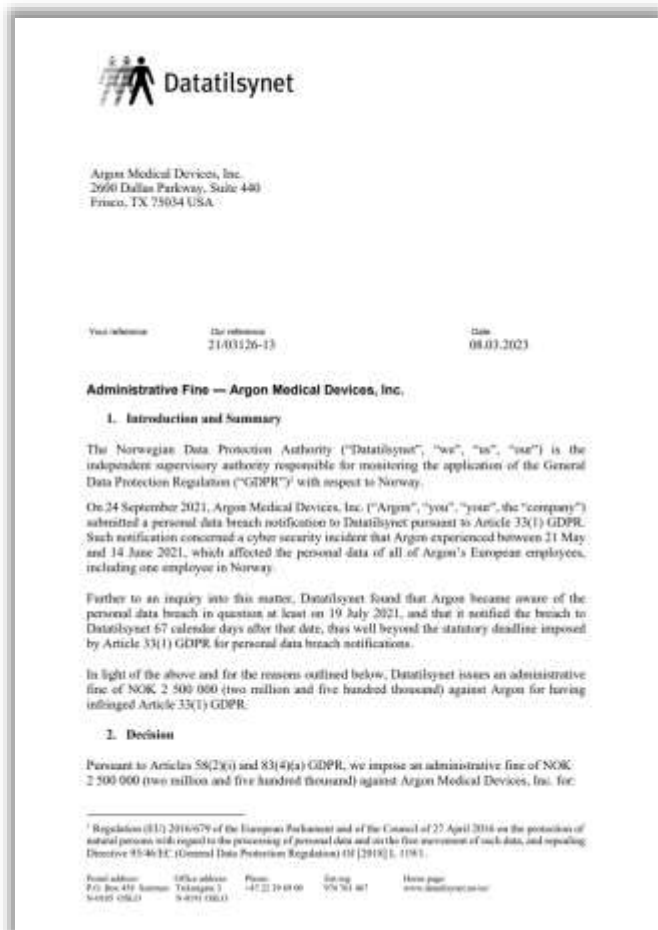
**За что:** нарушение ст. 5(1)(с), 28(3) GDPR и ст.82 Закона №78-17 от 06.01.1978 "Об обработке данных, файлах данных и свободах личности"

**Как:** штраф €125,000

**Причина:** скутеры Cityscoot оснащены бортовыми устройствами определения местоположения, которые позволяют пользователям через мобильное приложение знать местоположение скутера. В во время аренды скутера частным лицом Cityscooter собирает геолокационные данные каждые 30 секунд и сохраняет историю поездок скутеров. Cityscooter собирает геолокационные данные для борьбы с нарушениями правил дорожного движения, рассмотрения жалоб клиентов, поддержки пользователей, а также в целях кражи и управления, но ни одна из этих заявленных целей не требовала такого навязчивого использования геолокационных данных, какое практиковала Cityscoot.

Контракты Cityscoot с субподрядчиками не содержали всей информации, которая должна быть включена в соответствии с GDPR, например, требований, касающихся мер безопасности. Кроме того, Cityscoot использовала механизм reCAPTCHA, предоставленный Google, для своего мобильного приложения, который собирал данные приложения и передавал их Google для анализа в отсутствие информирования пользователей и получения их согласия.

## Штраф за неоправданную задержку в уведомлении о нарушении безопасности персональных данных



**Кто:** Datatilsynet (Норвегия)

**Кого:** Argon Medical Devices, Inc.

**Когда:** 2023.03

**За что:** нарушение ст. 33(1) GDPR

**Как:** возможный штраф €220,000

**Причина:** Компания Argon Medical Devices, расположенная в США, пострадала от инцидента кибербезопасности, после чего Datatilsynet получил сообщение от юридической фирмы от имени Argon Medical Devices, в котором говорилось, что последняя столкнулась с инцидентом, затрагивающим персональные данные всех сотрудников Argon Medical Devices в Европе, включая одного сотрудника в Норвегии. Argon Medical Devices стало известно о нарушении персональных данных не менее чем за 67 календарных дней до отправки уведомления в Datatilsynet.

Отчет компании Argon Medical Devices о том, как она справилась с нарушением и как она будет справляться с нарушениями в целом, выявил некоторые из возможных первопричин неадекватности принятых компанией мер. Например, Argon Medical Devices систематически и в значительной степени полагается на внешних консультантов, чтобы определить, следует ли сообщать о нарушении персональных данных в Европе. Такая модель соблюдения требований обычно замедляет процесс уведомления о нарушении, в частности, если она не сопровождается четкими инструкциями внешним консультантам о сроках проведения оценки, которые обязательно должны быть короче 72 часов, чтобы компания могла уложиться в срок, предусмотренный ст.33(1) GDPR.

## 923 Штраф за ненадлежащую санитизацию данных



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Azienda Sanitaria Locale della Provincia di Bari ('ASL')

**Когда:** 2023.03

**За что:** нарушение ст. 5(1)(a), 5(1)(c), 5(1)(f), 9, 25(1), 25(2) GDPR

**Как:** штраф €50,000

**Причина:** на странице "О нас говорят" сайта ASL были опубликованы отзывы, полученные ASL от бывших пациентов. Через вышеупомянутую страницу можно было получить доступ к сотням документов о пациентах, что позволяло третьим лицам идентифицировать их авторов, а также получить доступ к содержащимся в них персональным данным, поскольку такая информация была санитизирована ненадлежащим образом (с помощью черного маркера), что не препятствовало прочтению затемненных частей.

## Штраф за незаконную обработку персональных данных с помощью систем видеонаблюдения



**Chi:** Garante per la protezione dei dati personali (Italia)

**Chi:** H&M Hennes & Mauritz s.r.l.

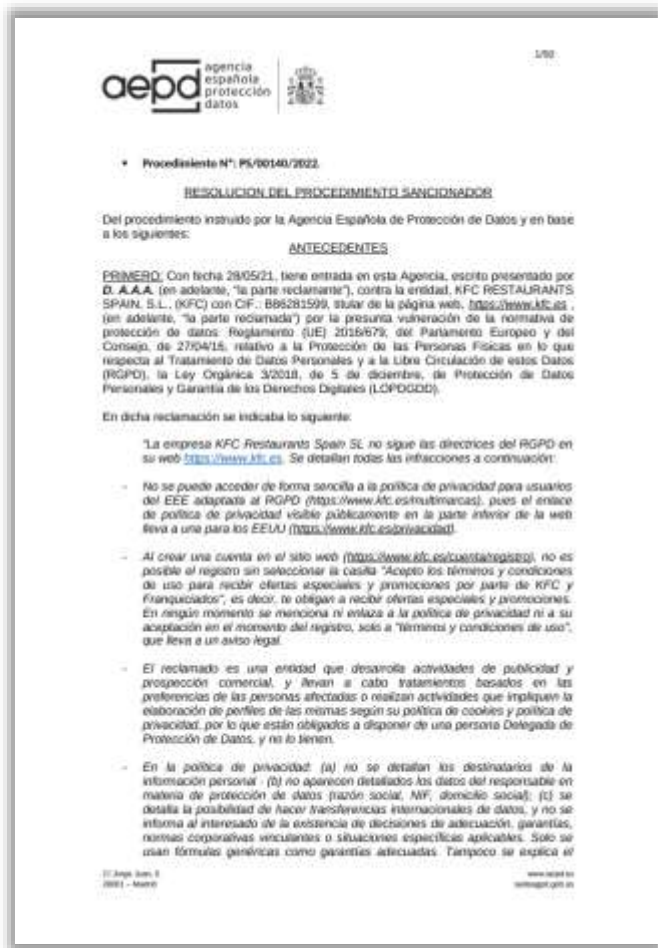
**Quando:** 2023.03

**Perché:** violazione art. 5(1)(a) GDPR

**Quanto:** multa €50,000

**Perché:** negozi H&M erano equipaggiati con telecamere di sorveglianza in aree riservate ai dipendenti. H&M giustificava l'installazione delle telecamere con la necessità di protezione contro i furti e la garanzia della sicurezza dei dipendenti. L'installazione di sistemi di sorveglianza veniva effettuata senza il consenso dei dipendenti o l'autorizzazione dell'ispezione del lavoro.

## Штраф за неназначение DPO и отсутствие информации в политике конфиденциальности



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** KFC Restaurants Spain S.L.

**Когда:** 2023.04

**За что:** нарушение ст. 13, 37 GDPR

**Как:** штраф €25,000 и один месяц на устранение нарушений

**Причина:** деятельность KFC была проверена по жалобе субъекта данных. В ходе проверки было установлено, что KFC не назначила ответственного за защиту данных (DPO) и не раскрыла информацию об обработке данных (например, о получателях персональных данных) в своей политике конфиденциальности, включив в нее вместо этого только общую и абстрактную информацию.



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Ediscom S.p.a.

**Когда:** 2023.04

**За что:** нарушение ст. 5(1)(a), 5(1)(b), 5(1)(c), 5(2), 6, 6(1)(a), 7, 7(2), 14, 24, 25 GDPR

**Как:** штраф €300,000 + несколько предписаний и запретов

**Причина:** неправомерные маркетинговые практики компании Ediscom при проведении рекламных кампаний посредством SMS-сообщений, электронных писем и автоматических звонков, в рамках которой использовалась база данных, содержащая персональные данные 21 миллиона человек. Она состояла из данных, собранных непосредственно Ediscom через различные онлайн-порталы (с помощью новостей, призовых конкурсов, тривиалов, кулинарных рецептов), а также из персональной информации, приобретенной у брокеров данных.

На некоторых своих порталах компания Ediscom использовала темные паттерны (dark patterns), которые с помощью соответствующим образом оформленных графических интерфейсов и других потенциально вводящих в заблуждение методов завлекали пользователей дать свое согласие на обработку данных в маркетинговых целях и на передачу данных третьим лицам с той же целью.

## 927 Штраф за неправильное обращение с данными об абортах



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** AMA S.p.A.

**Когда:** 2023.04

**За что:** нарушение ст. 28, 29, 32 GDPR

**Как:** штраф €239,000 + предписания в адрес муниципалитета "Рома Капитале" и управления здравоохранения "Рома 1".

**Причина:** на кладбище Фламинио в муниципалитете Рома Капитале, находящемся в ведении AMA, были установлены сотни белых крестов над могилами, где были захоронены плоды, и наклеены этикетки, раскрывающие данные женщин, прошедших процедуру прерывания беременности. Местное управление здравоохранения Roma 1 передало в AMA документацию с идентификационными данными женщин, которые затем были внесены в реестры кладбищ, что потенциально привело к риску получения персональных данных всех женщин, перенесших прерывание беременности во всех больницах района. Более того, личные данные женщин были также указаны на крестах, несмотря на то, что законодательство предусматривает, что при установке табличек на надгробиях указывается только информация об умершем.

## 928 Штраф за доступ к служебной электронной почте бывших работников



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** GEICO S.p.A.

**Когда:** 2023.04

**За что:** нарушение ст. 5(1), 13 GDPR

**Как:** штраф €40,000

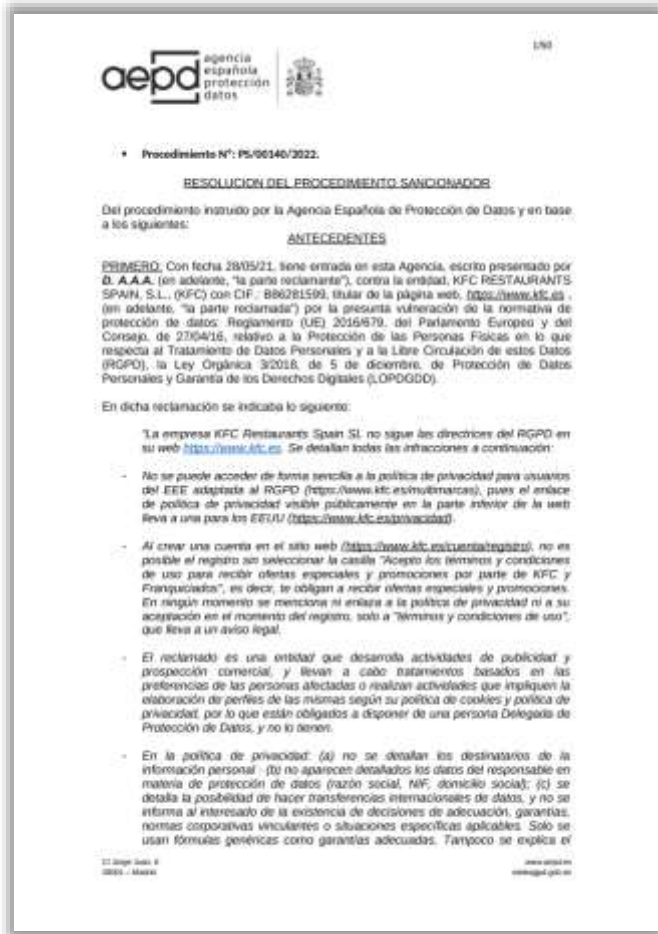
**Причина:** учетные записи электронной почты трех работников были деактивированы вскоре после их увольнения. Однако контроллер не заархивировал их, и перенаправил входящую почту на другую учетную запись. Субъекты данных заметили, что кто-то неоднократно получал доступ к их электронным почтовым ящикам даже после прекращения трудовых договоров благодаря автоматизированной системе оповещения о безопасности.

Контроллер утверждал, что доступ к учетным записям электронной почты уволенных работников был необходим для сбора информации для отдельного иска против них, поскольку они демонстрировали подозрительное поведение, которое могло потенциально нанести ущерб контроллеру. Субъекты данных были проинформированы в нескольких сообщениях о рабочих процедурах и политике компании, касающихся, в частности, ИТ-инструментов и услуг.

Было установлено, что уведомления работников не содержали информации об операциях по обработке данных, выполняемых контроллером после прекращения трудовых отношений. Кроме того, субъектам данных было дано понять, что их почтовые аккаунты больше не активны, а их сообщения больше не обрабатываются. Контроллер не смог представить доказательства того, что субъекты данных вели себя подозрительно, что оправдывало поведение контроллера. Кроме того, во внутренних правилах контроллера не была установлена продолжительность обработки данных.

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9909235>





**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** GSMA, Ltd. - организатор Mobile World Congress (Всемирный мобильный конгресс) в Барселоне

**Когда:** 2023.05

**За что:** нарушение ст. 35 GDPR

**Как:** штраф €200,000

**Причина:** от докладчика на MWC, гражданина Великобритании, потребовали предоставить скан-копию его паспорта - хотя докладчик планировал выступить на мероприятии в дистанционном режиме. Выяснилось, что GSMA создала систему идентификации для очных участников MWC, которая позволяла получить доступ на MWC на основе распознавания лиц и биометрических жетонов, управляемых компьютерной программой под управлением подрядчика GSMA. При этом GSMA предварительно не провела оценку воздействия системы на защиту данных участников MWC, не оценила соразмерность и необходимость внедрения системы и ее влияние на права и свободы субъектов данных.

## Штраф за незаконную обработку персональных данных из нелегально купленной базы данных



**Кто:** Agencija za zaštitu osobnih podataka (Хорватия)

**Кого:** B2 Kapital d.o.o.

**Когда:** 2023.05

**За что:** нарушение ст. 6(1), 13(1), 28(3), 32(1)(b), 32(2) GDPR

**Как:** штраф €2,265,000

**Причина:** компания B2 Kapital приобрела базу с данными 77,317 лиц, имеющих непогашенные долги перед кредитными учреждениями, включая их имена, фамилии и даты рождения. При этом B2 Kapital не проинформировала субъектов об обработке их персональных данных и соответствующем правовом основании для обработки. Кроме того, B2 Kapital не приняла соответствующие технические и организационные меры защиты данных и, скорее всего, даже не заметила бы утечку этих данных.

## 931 Штраф за псевдонимизацию вместо анонимизации

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Doctissimo (веб-сайт, где размещаются статьи, тесты, викторины и дискуссионные форумы, связанные со здоровьем и благополучием)

**Когда:** 2023.05

**За что:** нарушение ст. 5(1)(e), 9(2), 26 и 32 GDPR и ст.82 Закона №78-17 от 06.01.1978 "Об обработке данных, файлах данных и свободах личности"

**Как:** штраф €380,000

**Причина:** компания хранила персональные данные субъектов, включая их IP-адрес, наряду с любой информацией, введенной субъектами, в течение 24 месяцев после завершения тестов. Компания анонимизировала личные данные пользователей только после трех лет бездействия на сайте, и введенные процедуры представляли собой псевдонимизацию, а не анонимизацию, что позволяло повторно идентифицировать субъектов данных.

Doctissimo не получила согласия пользователя на обработку чувствительных персональных данных, а именно данных о здоровье, введенных во время тестов и викторин. Хотя для получения согласия пользователя использовался чек-бокс, в анкетах не было специального предупреждения или механизма для получения согласия, чтобы убедиться, что человек был осведомлен и дал согласие на обработку своих медицинских данных.

Doctissimo использовала протокол HTTP, а не более безопасный протокол HTTPS, а также не предприняла достаточных мер для обеспечения безопасности хранения паролей, а метод хэширования, используемый для паролей, мог быть расшифрован.

Куки-файлы устанавливались на терминале пользователя сразу после того, как он попал на главную страницу сайта Doctissimo, и что некоторые из этих куки-файлов были предназначены для целевой рекламы. Кроме того, CNIL пояснил, что, хотя у пользователей была возможность отказаться от всех файлов cookie, файлы cookie, которые уже были размещены, все равно хранились на терминале пользователя.

## Штраф за «неадекватное реагирование» на запрос клиента о своих персональных данных



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Volkswagen Leasing GmbH

**Когда:** 2023.05

**За что:** нарушение ст. 12, 15 GDPR

**Как:** штраф €40,000

**Причина:** Volkswagen отказал заявителю предоставить кредит для аренды автомобиля. При этом компания не предоставила никакой информации о персональных данных клиента, которые обрабатывались для оценки его кредитоспособности, отметили в ведомстве.

## 933 Штраф за неправомерный Интернет-таргетинг

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Criteo

**Когда:** 2023.06

**За что:** нарушение ст. 7(1), 7(3), 12, 13, 15(1), 17(1), 26 GDPR

**Как:** штраф €40,000,000

**Причина:** жалоба Privacy International и None of Your Business (NOYB) на компанию Criteo, которая специализируется на "поведенческом ретаргетинге" и собирает данные о просмотре сайтов интернет-пользователей с помощью своего трекера (cookie), который размещается на их терминалах при посещении определенных партнерских сайтов.

Трекер Criteo, используемый для таргетирования рекламы, размещался (в т.ч. партнерами Criteo) на пользовательских устройствах без согласия пользователей. Хотя получение согласия является обязанностью партнеров Criteo, которые находятся в непосредственном контакте с интернет-пользователями, Criteo все же обязана проверять и быть в состоянии продемонстрировать, что интернет-пользователи дали свое согласие. Criteo не приняла никаких мер для обеспечения того, чтобы ее партнеры действительно получали согласие интернет-пользователей, данные которых она затем обрабатывала. Контракты, заключенные Criteo и ее партнерами, не содержали никаких положений, обязывающих их предоставлять доказательства наличия согласия интернет-пользователей.

При назначении штрафа CNIL учитывал, что обработка касалась очень большого количества людей и что компания собрала очень большой объем данных, относящихся к поведению потребителей. Кроме того, во внимание был принят тот факт, что обработка данных физических лиц без подтверждения их действительного согласия позволила Criteo необоснованно увеличить число отслеживаемых лиц и, таким образом, финансовые доходы, которые она получает от своей роли рекламного посредника.

## Штраф за отсутствие прозрачности при автоматизированном принятии решений



**Кто:** BDI Berliner (Германия)

**Кого:** Deutsche Kreditbank

**Когда:** 2023.05

**За что:** нарушение ст.5(1)(a), 15(1)(h) и 22(3) GDPR

**Как:** штраф €300,000

**Причина:** клиент банка подал заявку на получение кредитной карты, в по результатам рассмотрения которой алгоритм банка отклонил её без какого-либо конкретного обоснования. В связи с этим банк предоставил клиенту только общую информацию о процессе скоринга в связи с его заявкой, когда его об этом попросили, и не предоставил никакой конкретной информации в отношении заявки клиента. Поэтому клиент не мог оспорить автоматизированное решение, принятое банком. Надзорный орган пришел к выводу, что непредоставление банком прозрачной и понятной информации об автоматизированном решении об отклонении заявления клиента, когда оно было запрошено.

## 935 Штраф за передачу персональных данных пользователей ЕС в США

**Кто:** Data Protection Commission (Ирландия)

**Кого:** Deutsche Kreditbank

**Когда:** 2023.05

**За что:** нарушение ст.5(1)(a), 15(1)(h) и 22(3) GDPR

**Как:** штраф €1,200,000

**Причина:** решение комиссии учитывает тот факт, что Meta Ireland нарушила статью 46 европейского закона о защите данных GDPR, продолжив передавать ПД из ЕС/Европейской экономической зоны (ЕЭЗ) в США после вынесения решения Суда Европейского союза по делу ирландского подразделения Facebook и иска австрийского юриста Макса Шремса (Max Schrems).

«Хотя Meta Ireland осуществляла передачу данных на основе обновлённых стандартных договорных положений (standard contractual clauses, SCC), принятых Еврокомиссией в 2021, в связке с дополнительными мерами, комиссия пришла к выводу, что эти действия не устраняют угрозы фундаментальным правам и свободам субъектов ПД, которые были идентифицированы Судом ЕС в его решении», – отметил регулятор.

Комиссия также потребовала от Meta приостановить любую дальнейшую передачу ПД европейцев в США в течение пяти месяцев с даты уведомления о решении регулятора Meta Ireland.

Кроме того, Meta должна привести свои операции по обработке [данных] в соответствие с положениями GDPR. В частности, прекратить незаконную обработку, включая хранение, в США персональных данных пользователей из ЕС/ЕЭЗ, переданных в нарушение GDPR в течение шести месяцев со дня получения соответствующего уведомления.

## 936 Штраф за отсутствие прозрачности в privacy notice

**IMY** Integritetsmyndigheten

1000

Spotify AB  
Regeringsgatan 16  
11152 Stockholm

Dokumentnummer:  
D-2019-0006

**Beslut efter tillsyn enligt  
dataskyddsförordningen – Spotify AB**

Datum:  
2023-06-12

**Innehållsförteckning**

Integritetsmyndighetens beslut	3
Spotify:s generella rutiner för hantering av begäran om tillgång	3
Granskning av skickade klagomål	3
1 Retorsgranskning för tillägsärendet	5
2 Tillägsärendets bestämmelser	6
3 Spotify:s generella rutiner för hantering av begäran om tillgång - Motivering av beslut	7
3.1 Information - artikel 15.1 a-h och 15.2 i dataskyddsförordningen	7
3.1.1 Vad som hänkommit i ärendet	7
3.1.2 Integritetsmyndighetens bedömning	8
3.2 Rätten till tillgång till personuppgifter och kopier på personuppgifter under behandling - artikel 15.1 och 15.3 i dataskyddsförordningen	12
3.2.1 Vad som har hänkommit i ärendet	12
3.2.2 Integritetsmyndighetens bedömning	16
4 Granskning av skickade klagomål - Motivering av beslut	20
4.1 Klagomål 1 (hän Norderländerna med nationellt referensnummer 22018-28413)	20
4.1.1 Bakgrund	20
4.1.2 Vad som har hänkommit i ärendet	20
4.1.3 Integritetsmyndighetens bedömning	22
4.2 Klagomål 2 (hän Dalerne med nationellt referensnummer D130.138)	23
4.2.1 Bakgrund	23
4.2.2 Vad som har hänkommit i ärendet	23
4.2.3 Integritetsmyndighetens bedömning	24
4.3 Klagomål 3 (hän Danmark med nationellt referensnummer 2018-31-119428)	24
5 Val av ingripande	26

Postadress:  
Box 8116  
104 20 Sönderborg

Webbplats:  
www.imy.se

E-post:  
mynd@imy.se

Telefon:  
08-687 81 80

**Кто:** Integritetsmyndigheten (Швеция)

**Кого:** Spotify

**Когда:** 2023.06

**За что:** нарушение ст.12(1), 15(1), 15(2) GDPR

**Как:** штраф €4,980,000

**Причина:** Spotify предоставляет информацию об осуществлении прав субъектов данных на 21 различных языках в своем уведомлении о конфиденциальности - в зависимости от языковых настроек используемого браузера. Информация в уведомлении о конфиденциальности не соответствовала требованиям прозрачности и не была адаптирована в зависимости от того, какими услугами решил воспользоваться субъект данных, например, какие категории персональных данных обрабатываются, получатели и где были собраны персональные данные, как долго данные будут храниться.

Spotify разделила персональные данные, предоставляемые субъектам данных, на различные уровни детализации. Следовательно, предоставление субъекту его персональных данных базового уровня детализации рискует привести субъекта данных к мысли, что такой объем персональных данных является их полной копией. Компания также не приняла достаточных мер для того, чтобы субъекты данных понимали описание обработки данных в нетехнических терминах, и что описание данных в технических лог-файлах по умолчанию предоставляется только на английском языке.



## 937 Штраф за нарушения при оказании услуг ясновидения

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Société KG COM

**Когда:** 2023.06

**За что:** нарушение ст. 5(1)(с), 6, 9, 12, 13, 28(3), 32, 33 GDPR и ст.82 Закона №78-17 от 06.01.1978 "Об обработке данных, файлах данных и свободах личности"

**Как:** штраф €150,000

**Причина:** компания KG COM управляет несколькими веб-сайтами для предоставления клиентам услуг по ясновидению. Среди нарушений компании:

- систематическая запись телефонных разговоров между телефонными операторами и потенциальными клиентами, а также между гадалками и клиентами с целью проверки качества и подтверждения факта заключения договора, без обеспечения минимизации собираемых и обрабатываемых персональных данных;
- хранение данных банковского счета клиента дольше, чем это было необходимо для завершения транзакции, борьбы с мошенничеством и последующих покупок;
- неполучение предварительного согласия от физических лиц на сбор специальных категорий персональных данных, таких как данные о здоровье и сексуальной ориентации;
- использование недостаточно надежных паролей для учетных записей пользователей, необеспечение защищенного доступа к использующим протокол http веб-сайтам, а также использование механизма шифрования банковских данных, который имел уязвимости;
- неуведомление о нарушении безопасности данных, связанного с процессором данных;
- незаключение договоров об обработке данных с несколькими процессорами данных, регулирующие отношения по обработке данных.

## 938 Штраф за нарушение принципа минимизации данных



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Sociedad Vascongada de Publicaciones, S.A.

**Когда:** 2023.06

**За что:** нарушение ст. 5(1)(c) GDPR

**Как:** штраф €90,000

**Причина:** согласно жалобе, поданной правительственной делегацией по борьбе с гендерным насилием, Sociedad Vascongada de Publicaciones опубликовала новостную статью и видео, содержащие личные данные 56 женщин, ставших жертвами гендерного насилия. Впоследствии Sociedad Vascongada de Publicaciones незамедлительно удалила видео по требованию AEPD и потребовала исключения из списка Google.

Характер нарушения был признан очень серьезным, так как оно подразумевало потерю контроля над персональными данными лиц, ставших жертвами гендерного насилия. Распространение этих данных создавало значительный риск их распознавания третьими лицами, что нанесло потенциальный вред пострадавшим лицам. Кроме того, число пострадавших лиц было признано значительным.

Несмотря на отсутствие намерения совершить нарушение, халатность была очевидна, поскольку СМИ не приняло адекватных мер по защите конфиденциальных персональных данных, особенно учитывая постоянную работу с данными пользователей.

## 939 Штраф за обработку данных на неверной правовой основе



**Кто:** Integritetsskyddsmyndigheten (Швеция)

**Кого:** Bonnier News AB

**Когда:** 2023.06

**За что:** нарушение ст. 6(1) GDPR

**Как:** штраф €1,103,000

**Причина:** 01.06.2022 компания Bonnier была ликвидирована путем слияния с компанией Expressen Lifestyle AB. Ранее Bonnier собирала персональные данные из баз данных всей группы для таких целей, как создание общего реестра клиентов, проверка правильности и актуальности данных, а также предоставление персональных данных дочерним компаниям для маркетинга собственных продуктов и услуг дочерних компаний. Информация, переданная в поведенческие базы данных, была собрана аффилированными компаниями Bonnier посредством файлов cookie, размещенных на терминалах пользователей.

Bonnier без согласия субъектов обрабатывала персональные данные для составления профиля субъектов данных и предоставляла такие профили партнерским компаниям для показа клиентам рекламы, а также предоставляла контактные данные клиентов партнерским компаниям для целей телефонного маркетинга и прямого маркетинга.

## 940 Штраф за незаконную практику веб-скрейпинга



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** владелец сайта trovanumeri.com

**Когда:** 2023.06

**За что:** нарушение ст. 5(1)(a), 5(1)(d), 5(2), 6, 12(1), 12(2), 13, 15, 16, 17, 24, 25 GDPR

**Как:** штраф €60,000

**Причина:** поступление жалоб от лиц, чьи данные были опубликованы, никогда не предоставляли своего разрешения – на сайте незаконно распространялись телефонные номера через справочник, созданный с помощью методов веб-скреппинга.

Владелец сайта не имел надлежащего правового основания для обработки данных, что на сайте отсутствовала информация, необходимая для связи с контролером данных, и что на этом же сайте отсутствовал какой-либо метод запроса на удаление персональных данных.

## 941 Штраф за смешение данных пациентов



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Camedì S.R.L.

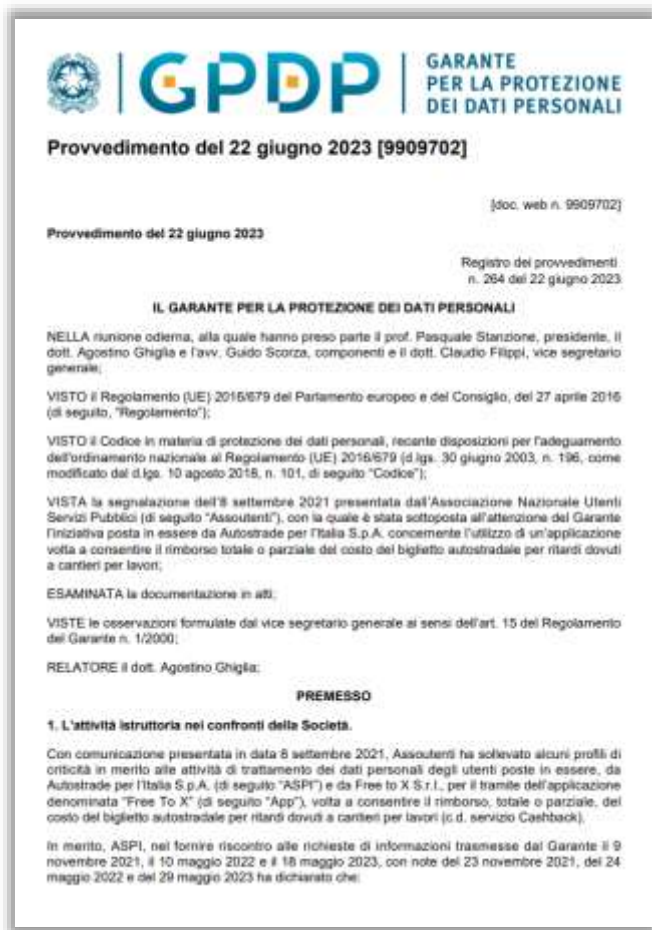
**Когда:** 2023.06

**За что:** нарушение ст. 5(1)(d), 5(1)(f), 5(2), 9, 32 GDPR

**Как:** штраф €10,000

**Причина:** компания Camedì перепутала данные двух пациентов с одинаковым именем в своей базе данных, что привело к неправильному указанию налогового кода и адреса проживания при доставке некоторых счетов, а также к отправке автоматических SMS-сообщений заявителю, а не пациенту, которому они были адресованы.

## 942 Штраф за неправильно составленный data processing agreement



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Autostrade per l'Italia S.p.A. (ASPI)

**Когда:** 2023.06

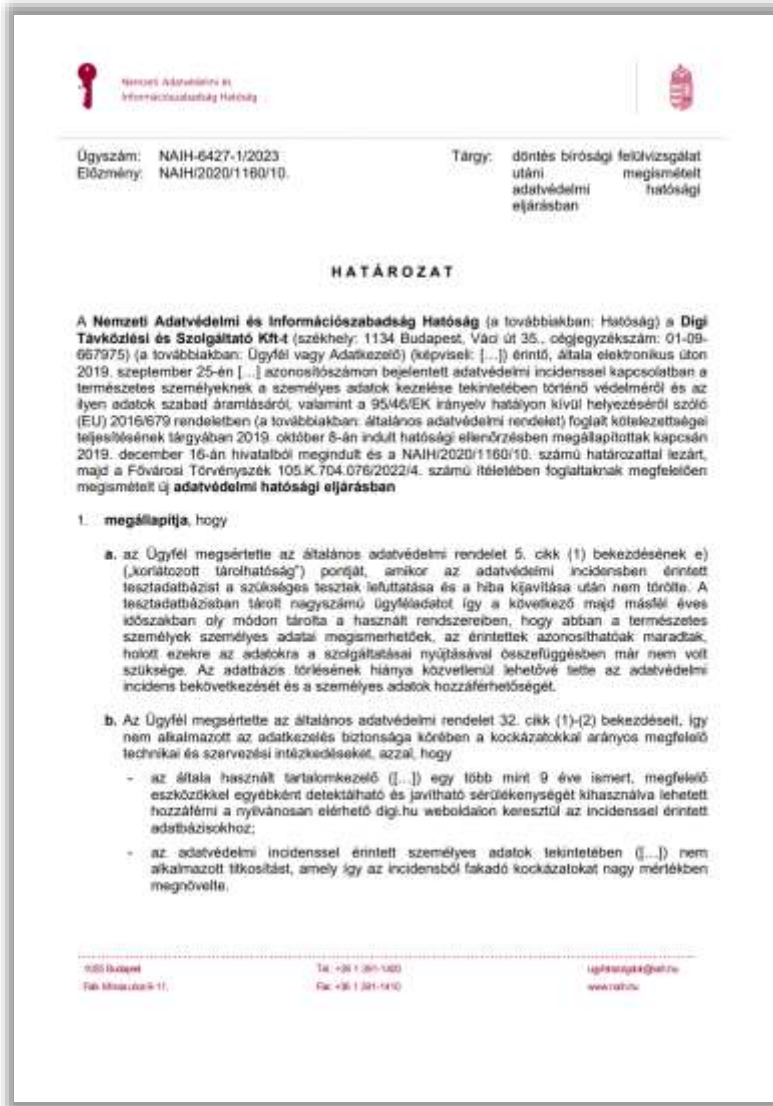
**За что:** нарушение ст. 5(1)(a), 13, 28 GDPR

**Как:** штраф €1,000,000

**Причина:** ассоциация потребителей Assoutenti пожаловалась на приложение ASPI для возмещения расходов на проезд, разработанным компанией Free To X S.r.l., которое позволяет возмещать стоимость билетов на автомагистрали за задержки, вызванные дорожными работами.

В соглашении об обработке данных между ASPI и Free to X S.r.l. ASPI была неверно указана в качестве обработчика данных, а не контроллера данных. Неправильная квалификация ролей двух компаний повлияла на уведомление о конфиденциальности информации, предоставляемое пользователям, которое, таким образом, было сформулировано некорректно. Кроме того, ASPI нарушила свое обязательство назначить Free To X в качестве обработчика данных. Таким образом, ASPI незаконно обработала персональные данные примерно 100,000 субъектов данных.

## 943 Штраф за утечку персональных данных на веб-сайте



**Кто:** Nemzeti Adatvédelmi és Információszabadság Hatóság (Венгрия)

**Кого:** Digi Telecommunications and Services Ltd.

**Когда:** 2023.06

**За что:** нарушение ст. 5(1)(a), 32(1), 32(2) GDPR

**Как:** штраф €205,000

**Причина:** в результате несанкционированного доступа к персональным данным субъектов персональных данных (например, клиентов и подписчиков новостной рассылки) через веб-сайт контроллера произошла утечка данных. В ходе расследования надзорный орган установил, что контроллер не принял надлежащих технических и организационных мер по защите персональных данных, что способствовало возникновению подобного инцидента.

## 944 Штраф за незаконное дистанционное наблюдение за сотрудниками



**Chi:** Garante per la protezione dei dati personali (Italia)

**Chi:** Ew Business Machines S.p.A. (Ew)

**Quando:** 2023.07

**Perché:** нарушение ст. 5(1)(a), 5(1)(c), 9, 13, 88 GDPR

**Как:** штраф €20,000

**Причина:** компания Ew установила на своих объектах систему сигнализации, активация и деактивация которой основана на использовании отпечатков пальцев, систему видеонаблюдения и приложение для геолокации некоторых своих сотрудников.

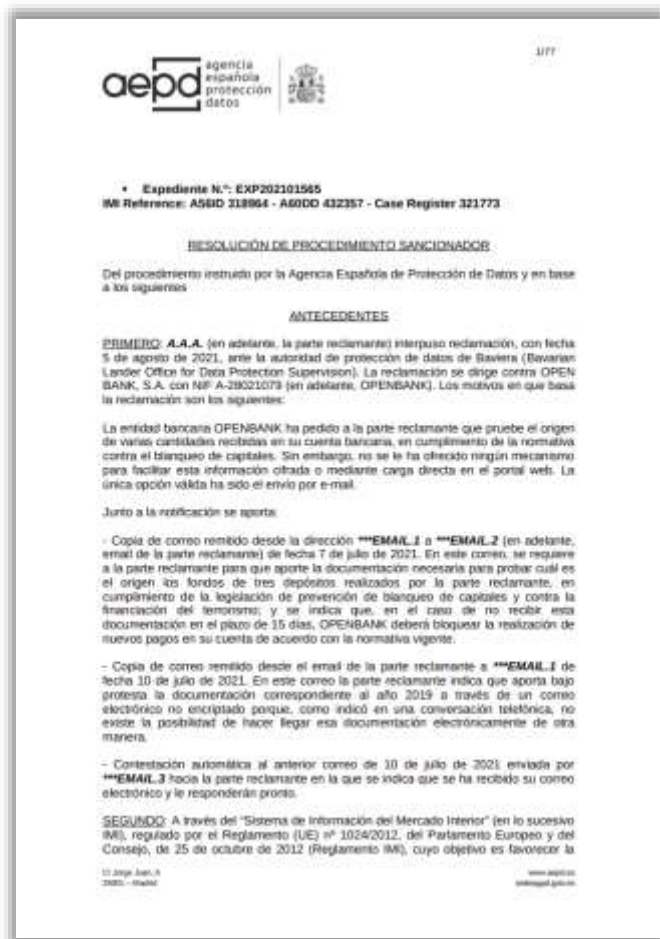
Чтобы обработка биометрических данных на рабочем месте была законной, она должна быть необходима для выполнения обязательств и реализации конкретных прав контролера данных или заинтересованной стороны в области трудового права.

GPS-геолокации сотрудников Ew осуществлялся с массовым, продолжительным и неизбирательным контролем деятельности работников.

Ew нарушила обязательства по предоставлению информации и принципы справедливости и законности обработки при использованием системы видеонаблюдения, основанной на непрерывной записи изображений и звуков через смартфоны, имеющиеся у сотрудников Ew, которые не были должным образом проинформированы о степени интрузивности наблюдения.



## 945 Штраф за направление документов по электронной почте



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Open Bank, S.A.

**Когда:** 2023.07

**За что:** нарушение ст. 25, 32 GDPR

**Как:** штраф €2,500,000

**Причина:** клиенту банка было предложено доказать происхождение денежных средств, поступивших на его банковский счет, в соответствии с правилами противодействия отмыванию денег. Однако банк не предложил никакого механизма, способствующего предоставлению такой информации в защищенном виде, например, путем шифрования информации или загрузки ее на веб-портал, и вместо этого попросил направить документы по электронной почте.

## 946 Штраф за неправильную анонимизацию медицинских данных



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Thin S.r.l.

**Когда:** 2023.07

**За что:** нарушение ст. 5(1)(a), 9(2), 13 GDPR

**Как:** штраф €15,000

**Причина:** компания Thin участвовала в реализации международного проекта, направленного на улучшение качества обслуживания пациентов путем сбора и анализа данных о состоянии здоровья. Терапевты, участвующие в проекте, должны были добавить в используемую систему управления (называемую "Medico 2000" и поставляемую ИТ-компанией, работающей в партнерстве с Thin) дополнительный функционал, который автоматически анонимизировал бы данные пациентов и передавал их в базу данных, принадлежащую Thin. Взамен врачи общей практики могли получить льготы, в том числе и финансовую компенсацию.

Дополнительный функционал в системе не позволял эффективно анонимизировать медицинские данные, т.к. простая замена идентификатора, присвоенного пациентам, системой шифрования или необратимым хэш-кодом ни при каких обстоятельствах не является надлежащей мерой в отношении требования об устранении особенностей, необходимых для квалификации операции обработки как анонимизации.

Таким образом, компания Thin основывалась на ошибочном предположении, что она обрабатывает анонимизированные данные, она фактически незаконно обрабатывала псевдонимизированные персональные данные.

## Штраф за непредоставление бывшему работнику доступа к отчету о дисциплинарном расследовании



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** AcegasApsAmga S.p.A.

**Когда:** 2023.07

**За что:** нарушение ст. 5(1)(a), 12, 15 GDPR

**Как:** штраф €10,000

**Причина:** бывший сотрудник компании AcegasApsAmga, не смог получить полный ответ на запросы о доступе к своим персональным данным, поданные после получения дисциплинарного взыскания, содержащего подробные ссылки на нерабочую деятельность, которая привела к увольнению сотрудника.

В ответ на несколько запросов субъекта компания AcegasApsAmga ответила, что запросы носят слишком общий характер и что необходимо подробно указать информацию, к которой запрашивается доступ. Только спустя почти год после первого запроса о доступе бывшему сотруднику стало известно о существовании и содержании отчета о расследовании, на основании которого было вынесено дисциплинарное взыскание.

Надзорный орган определил, что компания AcegasApsAmga должна была предоставить заявителю все данные, собранные в отчете о расследовании, включая информацию, которая не была включена в дисциплинарное уведомление, например, фотографии и данные GPS, в соответствии со статьями 12 и 15 GDPR. В этой связи Гарант подчеркнул, что незаконно утаенные данные могли бы быть полезны для осуществления права на защиту.



**Кто:** Urząd Ochrony Danych Osobowych (Польша)

**Кого:** неназванная компания

**Когда:** 2023.07

**За что:** нарушение ст. 5(2), 33(1), 34(1) GDPR

**Как:** штраф €2,640

**Причина:** в мае 2022г. контролер, владелец местного бизнеса, стал жертвой утечки данных. С его компьютера был похищен файл, содержащий персональные данные клиентов. Похищенные данные включали имена, домашние и электронные адреса, номера телефонов и национальные идентификационные номера субъектов данных.

Контролер проинформировал об этом инциденте DPA Польши, но не сообщил никаких подробностей о том, были ли субъекты данных проинформированы о нарушении данных и существует ли в результате этого какой-либо риск для их прав и свобод. Более того, контроллер обратился в DPA по истечении 72-часового периода. Хотя DPA запросил у контролера разъяснения, но не получил от него ответа.

## Штраф за незаконную обработку медицинских данных персонала в связи с возможным расторжением трудовых договоров



Berliner Beauftragte  
für Datenschutz  
und Informationsfreiheit

### Pressemitteilung

711.412.1

5. November 2019

#### Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft

Am 30. Oktober 2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) erlassen.

Bei Vor-Ort-Prüfungen im Juni 2017 und im März 2019 hat die Aufsichtsbehörde festgestellt, dass das Unternehmen für die Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendete, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen. Es handelte sich dabei um Daten zu den persönlichen und finanziellen Verhältnissen der Mieterinnen und Mieter, wie z. B. Gehaltsbescheinigungen, Selbstauskunftformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge.

Nachdem die Berliner Datenschutzbeauftragte im ersten Prüftermin 2017 die dringende Empfehlung ausgesprochen hatte, das Archivsystem umzustellen, konnte das Unternehmen auch im März 2019, mehr als ein Jahr nach dem ersten Prüftermin und neun Monate nach Anwendungsbeginn der Datenschutz-Grundverordnung weder eine Bereinigung ihres Datenbestandes noch rechtliche Gründe für die fortdauernde Speicherung vorweisen. Zwar hatte das Unternehmen Vorbereitungen zur Beseitigung der aufgefundenen Missstände getroffen. Diese Maßnahmen hatten jedoch nicht zur Herstellung eines rechtmäßigen Zustands bei der Speicherung personenbezogener Daten geführt. Die Verhängung eines Bußgeldes wegen eines

Pressesprecherin: Dalia Kues  
Geschäftsstelle: Cristina Vecchi  
E-Mail: [presse@datenschutz-berlin.de](mailto:presse@datenschutz-berlin.de)

Friedrichstr. 219  
10969 Berlin

Tel: 030 13889 - 900  
Fax: 030 2156050



**Кто:** BDI Berliner (Германия)

**Кого:** неназванная компания

**Когда:** 2023.08

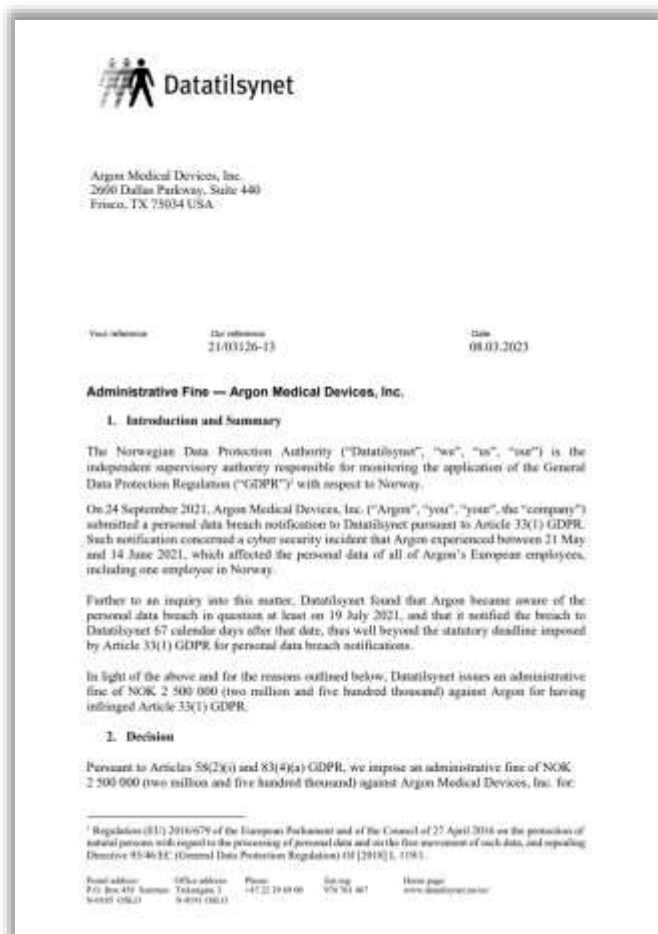
**За что:** нарушение ст. 5(1)(b), 9(2)GDPR

**Как:** штраф 215,000

**Причина:** компания вела базу данных со специальными категориями персональных данных своих сотрудников. База данных велась с целью выбора сотрудников для увольнения по окончании испытательного срока. Такая база данных включала в себя информацию о психологическом состоянии некоторых сотрудников, обращениях за психотерапией, а также их склонности к вступлению в профсоюз.

Компания незаконно обрабатывала специальные категории данных, включая данные о здоровье, так как договор между работодателем и сотрудниками не может быть действительным правовым основанием для рассматриваемой обработки. При определенных обстоятельствах работодатель может потребовать от своих сотрудников предоставления определенных данных, в том числе и конфиденциальных. Тем не менее, рассматриваемые в данном случае действия по обработке, даже если они основывались на данных, предоставленных непосредственно работниками, не были необходимы в контексте договора и нарушали принцип ограничения цели.

## 950 Штраф за неправомерный сбор персональных данных норвежцев



**Кто:** Datatilsynet (Норвегия)

**Кого:** Meta Platforms Ireland Limited

**Когда:** 2023.08

**За что:** нарушение ст. 6(1)(b), 6(1)(f) GDPR

**Как:** штраф €89,000 в день

**Причина:** Meta не имеет права собирать данные пользователей, включая информацию о местоположении, и использовать эти данные для показа норвежцам таргетированной рекламы.

Надзорный орган предъявил Meta соответствующие претензии 17.07.2023 и дал срок на устранение нарушений до 04.08.2023. Требования Datatilsynet не были выполнены.

Datatilsynet планирует штрафовать Meta до 03.11.2023. Если компания откажется исполнять предписание надзорного органа, Datatilsynet может с санкции Европейского совета по защите данных (European Data Protection Board, EDPB) штрафовать американскую компанию неопределённо долго.

В случае поддержки решения норвежского регулятора со стороны EDPB за неправомерный сбор данных Meta могут начать штрафовать и другие страны Европы.

## Штраф за размещение сотрудником в социальных сетях видео, снятое системой видеонаблюдения компании

The screenshot shows the website of the National Authority for Data Protection (ANSPDCP) in Romania. The main heading is "Amendă pentru încălcarea RGPD" (Fine for GDPR violation). The text states that the authority has finalized an investigation into the operator BODY LINE SRL, which is fined for violating articles 5, 4, 9, 17, and 32 of the GDPR. The total fine is 49,322 lei, equivalent to 10,000 EUR. The violation involved the operator's failure to ensure data security and the dissemination of personal data on social media. The website also features a sidebar with navigation links for "Regulament (UE) 2016/679", "Plângeri", "Operatori", and "Schengen".

**Кто:** Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Румыния)

**Кого:** Body Line S.R.L.

**Когда:** 2023.08

**За что:** нарушение ст. 5, 6, 9, 17, 32(1), 32(2) GDPR

**Как:** штраф €10,000

**Причина:** компания разгласила персональные данные субъекта данных (клиента компании), разместив на страницах компании в социальных сетях аудиовидеозапись с системы видеонаблюдения.

Сотрудник компании распространил данные субъекта данных на своих страницах в социальных сетях, разместив аудиовидеозапись субъекта данных и указав ник субъекта данных, который раскрывал этническое происхождение субъекта данных.

Субъект данных подал запрос на удаление данных в соответствии со ст.17 GDPR, но он был проигнорирован.

## 952 Штраф за утечку данных из-за использования некорректных URL-адресов



**Кто:** Integritetsskyddsmyndigheten (Швеция)

**Кого:** Trygg-Hansa A/S (ранее - Moderna Försäkringar)

**Когда:** 2023.08

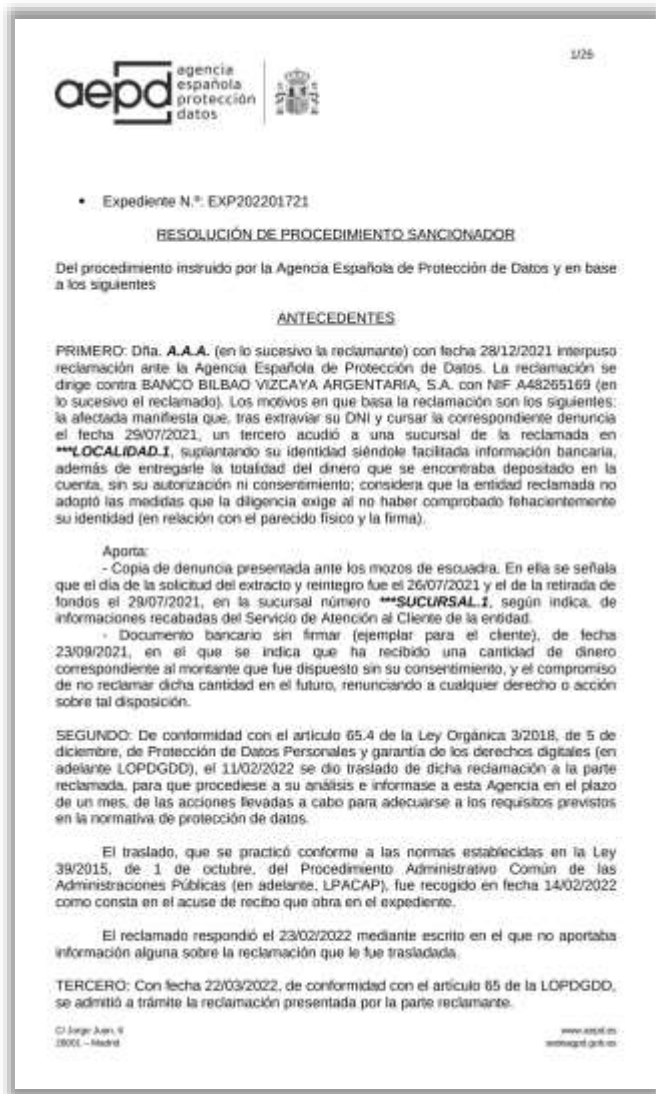
**За что:** нарушение ст. 5(1)(f), 32(1) GDPR

**Как:** штраф €3,000,000

**Причина:** в результате нарушения безопасности был получен доступ к персональным данным около 650,000 клиентов контролера данных, включая медицинскую, финансовую и контактную информацию. Нарушение безопасности было обнаружено, когда один из получателей электронного письма от Trygg-Hansa понял, что, изменив веб-ссылку, он может получить доступ к документам других клиентов без аутентификации. Данная уязвимость существовала более двух лет, с октября 2018 года по февраль 2021 года. Было установлено, что компания Trygg-Hansa не предприняла адекватных технических и организационных мер по защите персональных данных, что и позволило произойти подобному инциденту.



## 953 Штраф за непринятие эффективных мер идентификации



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Banco Bilbao Vizcaya Argentaria, S.A. (BBVA)

**Когда:** 2023.09

**За что:** нарушение ст. 6(1), 32(1) GDPR

**Как:** штраф €70,000

**Причина:** по утверждению заявителя, неизвестное лицо использовало его утерянное удостоверение личности, чтобы выдать себя за него и с помощью этой информации получить доступ к €9,400, находящимся на банковском счете заявителя.

BBVA не смогла правильно идентифицировать неизвестное лицо, запросившее снятие денег с банковского счета, поскольку не проверила соответствие внешности человека на удостоверении личности лицу, предъявившему его в отделении BBVA, и не удостоверилась, что подпись третьего лица соответствует данным заявителя, хранящимся в BBVA.

Также установлено, что BBVA не внедрила и не использовала соответствующие технические и организационные меры, гарантирующие уровень безопасности, соответствующий риску обработки.

## 954 Штраф за недостаточную защиту данных несовершеннолетних

**Кто:** Data Protection Commission (Ирландия)

**Кого:** TikTok Limited

**Когда:** 2023.09

**За что:** нарушение ст. 5(1)(c), 5(1)(f), 12(1), 13(1)(e), 24(1), 25(1) и 25(2) GDPR

**Как:** штраф €345,000,000 + предписание исправить нарушения

**Причина:** речь идет о нарушениях, отмеченных в период с 31 июля 2020 года по 31 декабря 2020 года. Представители TikTok не согласились с решением регулятора и суммой штрафа, указав на то, что перечисленные нарушения были устранены еще до начала расследования в сентябре 2021 года.

Среди выявленных нарушений:

- В настройках профилей детей-пользователей TikTok по умолчанию был установлен публичный режим, что позволяло любому желающему просматривать контент, размещаемый детьми-пользователями.
- При внедрении настройки учетной записи по умолчанию для детей, которая позволяла любому пользователю просматривать контент социальных сетей, размещенный детьми, не были учтены возможные риски для прав и свобод детей-пользователей.
- Была реализована настройка платформы под названием "Family Pairing" для пользователей-детей, в соответствии с которой пользователь, не являющийся ребенком, мог связать свой аккаунт с пользователем-ребенком, что позволяло осуществлять прямой обмен сообщениями между пользователями, не являющимися детьми, и пользователями-ребятами старше 16 лет.
- Детям-пользователям не была представлена информация о получателях или категориях получателей персональных данных, а также не была предоставлена информация об объеме и последствиях обработки изначально общедоступных данных в краткой, прозрачной и понятной форме.
- Приложение подталкивало пользователей выбирать менее жесткие настройки приватности при регистрации и загрузке видео. Это делалось с помощью так называемых темных паттернов (dark patterns) - особенностей интерфейса и работы приложения, из-за которых пользователю легче совершить действия, противоречащие его интересам.

[https://edpb.europa.eu/system/files/2023-09/final\\_decision\\_tiktok\\_in-21-9-1 - redacted 8 september 2023.pdf](https://edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf)

[https://edpb.europa.eu/news/news/2023/following-edpb-decision-tiktok-ordered-eliminate-unfair-design-practices-concerning\\_en](https://edpb.europa.eu/news/news/2023/following-edpb-decision-tiktok-ordered-eliminate-unfair-design-practices-concerning_en)



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Муниципалитет Модики

**Когда:** 2023.09

**За что:** нарушение ст. 5(1)(a), 5(1)(c), 5(1)(e), 5(2), 12, 13, 24, 25, 28, 37(1), 37(7) GDPR

**Как:** штраф €45,000

**Причина:** муниципалитет использовал систему видеонаблюдения (CCTV) для выявления административных нарушений из-за неправильной утилизации отходов, выявленную по видеозаписям камер видеонаблюдения. Обработка персональных данных с помощью систем видеонаблюдения государственными организациями в целом допустима, если это необходимо для выполнения юридического обязательства, отметив, что управление отходами является одним из видов деятельности, возложенной на местные органы власти.

Местные органы власти, как контролеры данных, обязаны соблюдать принципы защиты данных. Так, муниципалитет:

- не предоставил субъектам данных адекватной информации об обработке персональных данных с помощью камер видеонаблюдения;
- нарушил принципы минимизации данных, ограничения хранения, подотчетности и защиты данных по замыслу и по умолчанию;
- не определил своевременно отношения с двумя компаниями, с которыми был заключен договор на установку и обслуживание камер видеонаблюдения (эти компании также были оштрафованы на €10,000 и €5,000 евро соответственно);
- своевременно не назначил ответственного за защиту данных (DPO) и не опубликовал его контактные данные.

## 956 Штраф за удаление персональных данных

 DATATILSYNET

### Landsretten giver bøde på 1. mio. kr. til hotelkæde

Dato: 28-09-2023

Nyhed

Hotelkæden Arp-Hansen er blevet idømt en bøde på 1 mio. kr. af Østre Landsret. Dommen giver vigtig praksis på området.



Den 20. september 2023 [afsagde Østre Landsret dom](#) i en sag mod Arp-Hansen Hotel Group A/S om overtrædelse af databeskyttelsesforordningens regler om opbevaring af personoplysninger. Hotelkæden blev idømt en bøde på 1 mio. kr., hvilket ligger tæt på [Datatilsynets oprindelige bødestilling på 1,1 mio. kr.](#)

**Кто:** Datatilsynet (Дания)

**Кого:** Arp-Hansen Hotel Group A/S

**Когда:** 2023.09

**За что:** нарушение ст. 5(1)(e) GDPR

**Как:** штраф €135,000

**Причина:** компания Arp-Hansen сохраняла персональные данные клиентов дольше, чем это было необходимо после истечения установленных ею же сроков удаления. Ранее дело рассматривалось окружным судом, который признал Arp-Hansen нарушившей свои обязательства, но решил не налагать штраф. Впоследствии прокуратура подала апелляцию в Высокий суд, который также признал компанию Arp-Hansen нарушившей статью 5(1)(e) GDPR за то, что она не удалила персональные данные своих клиентов в соответствии с политикой хранения данных, разработанной самой компанией Arp-Hansen.

## Штраф за непарвомерную обработку сведений о личной жизни работников

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** SAF Logistics

**Когда:** 2023.09

**За что:** нарушение ст. 5(1)(с), 9(2), 10, 31 GDPR

**Как:** штраф €200,000

**Причина:** SAF Logistics является компанией, занимающейся авиаперевозками, материнская компания которой находится в Китае. В рамках внутреннего подбора персонала на должность в компании SAF Logistics собирала персональные данные, касающиеся личной жизни своих сотрудников. Так, все сотрудники получили анкеты на китайском языке для предоставления таких персональных данных, как этническая принадлежность, принадлежность к политической партии, семейное положение, а также имена родителей, братьев и сестер.

Компания хранила справки о судимости сотрудников даже после того, как соответствующие сотрудники были оправданы властями по результатам административного расследования.

Наконец, в отношении форм, предоставляемых сотрудникам и требующих предоставления конфиденциальных персональных данных, не был обеспечен корректный перевод таких форм. Из французских переводов форм, которые изначально были на китайском языке, были удалены поля, касающиеся этнической и политической принадлежности.

Несмотря на то, что 13.08.2020 компания SAF Logistics получила письмо от CNIL о запросе конфиденциальных персональных данных, SAF Logistics продолжала рассылать формы сотрудникам. Таким образом, CNIL определила, что заявления SAF Logistics противоречат ее действиям и демонстрируют нежелание сотрудничать с CNIL.



**Кто:** Agencija za zaštitu osobnih podataka (Хорватия)

**Кого:** неназванный отель

**Когда:** 2023.09

**За что:** нарушение ст. 6(1), 13(1), 13(2), 32(1)(a), 31(1)(d), 32(4), 38(6) GDPR

**Как:** штраф €15,000

**Причина:** при бронировании проживания в отеле через онлайн-форму подтверждение бронирования было запрошено путем отправки номера CVC кредитной карты по незащищенным каналам (т.е. по электронной почте) и необходимо также предоставить копию действительного документа, удостоверяющего личность, с фотографией.

Кроме того, отель не сообщил ясным и прозрачным образом об обработке персональных данных в документе "Общие положения и условия" на сайте отеля и не предоставил точную и полную информацию об обработке в форме согласия на использование персональных данных.

Отель не принял соответствующих технических и организационных мер, включая, в частности, шифрование персональных данных и внедрение процессов регулярного тестирования, оценки и анализа эффективности этих мер. Назначение менеджера отеля ответственным за защиту данных (DPO) нарушает статью 38(6) GDPR, отметив, что DPO может выполнять другие задачи и обязанности, однако такие задачи и обязанности не должны приводить к конфликту интересов.

# Штраф за нарушение правил безопасности и получения согласия на использование файлов cookie

**Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal**

Protejația Datelor | Data: 1

Informații generale | Legislație | Proceduri | Timpuri Internonaționale | Contact

Home » Comunicat\_Presa\_23.08.2023

N/04/2023 9:24 Română | English | Français

23.08.2023

### Amendă pentru încălcarea RGPD

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal a finalizat în luna iulie 2023 o investigație la operatorul BDDY LINE SRL și a constatat că acesta a încălcat prevederile art. 5, 4, 9, 17 și art. 32 alin. (1) și (2) din Regulamentul (UE) 2016/679 (GDPR).

Operatorul a fost sancționat contravențional cu amendă în cuantum total de 49.322 lei, echivalentul a 10.000 EURO.

Investigația a fost demarată ca urmare a unei plângeri prin care s-a reclamat divulgarea de către operator a datelor personale ale unei persoane (clicat al operatorului) prin postarea unei înregistrări audio-video pe pagina de socializare ale operatorului.

În cursul investigației efectuate Autoritatea Națională de Supraveghere a constatat că BDDY LINE SRL, prin intermediul paginilor sale de socializare, a divulgat datele personale din înregistrările audio-video și a fototit în comentarii un apelativ ce dezvăluie originea etnică a societății, fără a avea termenii legal, încălcându-se astfel prevederile art. 5, 6 și 9 din Regulamentul (UE) 2016/679.

De asemenea, s-a constatat că operatorul nu a dat curs cererii titularului de ștergere a datelor încălcând prevederile art. 17 din Regulamentul (UE) 2016/679.

În același timp, s-a constatat și faptul că operatorul nu a adoptat suficiente măsuri tehnice și organizaționale adecvate în vederea asigurării confidențialității datelor personale prelucrate prin intermediul sistemului de supraveghere audio-video.

Acasă în situație a condus la acțiunea și, ulterior, la divulgarea pe paginile de socializare ale operatorului a unei înregistrări audio-video cu imagini ale titularului, fiind astfel încălcată prevederile art. 32 alin. (1) și (2) din Regulamentul (UE) 2016/679.

Totodată, operatorul BDDY LINE SRL i a su aplicat și următoarele măsuri corective:

- de a asigura conformitatea cu GDPR a operațiunilor de prelucrare a datelor personale, inclusiv prin elaborarea de proceduri scrise, astfel încât datele personale ale persoanelor vizate să fie prelucrate cu strictă respectare a dispozițiilor legale privind protecția datelor personale, prin evitarea colectării și/sau divulgării ilegale/inecuvinte/inautorizate a datelor personale ale acestora;
- de a da curs cererii de ștergere a datelor personale ale titularului, oferindu-i posibilități de pe paginile de socializare ale operatorului;
- de a asigura conformitatea cu GDPR a operațiunilor de prelucrare a datelor personale, prin implementarea unor măsuri tehnice și organizaționale adecvate, în special sub aspect instruirii persoanelor care prelucratează date sub autoritatea sa (angajați sau colaboratori), prin organizarea regulată a unor sesiuni de instruire cu acestea, în legătură cu obligațiile ce le revin privind prelucrarea datelor personale prin intermediul sistemului de supraveghere video, al stabilirii condițiilor în care pot fi accesate imaginile sau înregistrările audio-video de către un număr redus de persoane, pe baza unor credențiale individuale, al verificării periodice a accesului la înregistrările audio-video, precum și al detectării rapide, gestionării și raportării unor situații de încălcare a securității datelor personale.

ANSPDPC

**Кто:** Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Румыния)

**Кого:** Restart Energy One SA

**Когда:** 2023.09

**За что:** нарушение ст. 32(1)(b), 32(1)(d), 32(2) GDPR, ст.4(5) Закона об электронных коммуникациях.

**Как:** штраф €33,000

**Причина:** файл с веб-сайта компании Restart Energy One, содержащий персональные данные по меньшей мере 750 субъектов данных, находился в открытом доступе по ссылке, выдаваемой поисковыми системами, в течение примерно двух с половиной лет. Кроме того, при доступе к веб-сайту Restart Energy One на устройство пользователя устанавливались файлы cookie, не являющиеся технически необходимыми, до того, как пользователь мог дать на них согласие. Кнопка "Отказаться" не остановлена установку файлов cookie на устройство пользователя.

## Штраф за незаконную обработку персональных данных из нелегально купленной базы данных



**Кто:** Agencija za zaštitu osobnih podataka (Хорватия)

**Кого:** EOS Matrix d.o.o.

**Когда:** 2023.10

**За что:** нарушение ст. 5(2), 6(1), 9(2), 12(1), 13(1), 13(2), 32(1)(b), 32(2) GDPR

**Как:** штраф €5,470,000

**Причина:** AZOP 22.03.2023 получил анонимное заявление о том, что компания EOS Matrix несанкционированно обработала большое количество персональных данных физических лиц (должников). К заявлению был приложен USB-накопитель, содержащий персональные данные 181 641 человека, из которых 294 на момент формирования базы были несовершеннолетними и содержали персональные данные, включая фамилию, имя, отчество, дату рождения и OIB, а также имели непогашенную задолженность перед первоначальными кредиторами, которые были приобретены компанией EOS Matrix.

Информация о том, что конкретное лицо находится в отношениях должника и кредитора с компанией EOS Matrix, наряду с другими персональными данными, не фиксируется ни в каких системах хранения с другими учреждениями, кроме системы EOS Matrix. AZOP заявил, что пока не установлено, каким именно образом была осуществлена утечка данных 181 641 субъекта, что речь идет о возможном уголовном преступлении в виде несанкционированного использования персональных данных, и отметил, что AZOP активно сотрудничает с Департаментом полиции Загреба и Муниципальной прокуратурой Загреба по этому вопросу.



## 961 Штраф за неправомерную рассылку маркетинговых сообщений



**Кто:** Integritetsskyddsmyndigheten (Швеция)

**Кого:** H&M Hennes & Mauritz GBC AB

**Когда:** 2023.10

**За что:** нарушение ст. 12(3), 21(3) GDPR

**Как:** штраф €30,000

**Причина:** рассылка компаний маркетинговых сообщений, несмотря на то, что субъекты данных воспользовались своим правом на возражение. Компания не располагала достаточными системами и процедурами, способствующими осуществлению права субъектов данных на возражение против прямого маркетинга.

## Штраф за заключение незапрошенных договоров, содержащих неверные персональные данные

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Axpo Italia S.p.A.

**Когда:** 2023.10

**За что:** нарушение ст. 5(1)(a), 5(1)(d), 5(2), 24 GDPR

**Как:** штраф €10,000,000 + предписание принять корректирующие меры

**Причина:** компания Axpo Italia приобретала новые контракты на поставку электроэнергии и газа через сеть из примерно 280 продавцов (агентов и субагентов), не имея соответствующих инструментов и процедур для обеспечения соответствия данных, вносимых продавцами в базу данных, реальным пользователям коммунальных услуг. Эти недостатки привели к заключению незапрошенных договоров, в которые зачастую вносились неточные и устаревшие персональные данные. Кроме того, базе данных Axpo Italia содержалось 2462 предложения о заключении договоров, в которых один и тот же адрес электронной почты потенциального клиента повторялся более пяти раз.

Учитывая серьезность нарушений, продолжительность незаконной обработки (около одного года и шести месяцев) и количество затронутых лиц (более 5 тыс.), Garante наложил существенный штраф и обязал компанию принять ряд корректирующих мер, в том числе:

- использование системы блокировки для проверки достоверности контрактов, приобретаемых через сеть продавцов;
- внедрение систем оповещения, позволяющих выявить любое неправомерное и/или мошенническое поведение продавцов при получении данных о потенциальных клиентах;
- внедрение механизмов, позволяющих удостовериться в фактическом получении сообщений, переданных клиенту на этапе заключения договора;
- принятие процессуальных норм, направленных на усиление аудиторской деятельности в отношении работы агентств.

Кроме того, Garante предписал прекратить дальнейшую обработку персональных данных клиентов, чьи контракты были расторгнуты в результате жалоб на нежелательные активации услуг.

## Штраф за незаконную обработку данных для маркетинга и несотрудничество с надзорным органом



**Chi:** Garante per la protezione dei dati personali (Italia)

**Chi:** Università e-Campus

**Quando:** 2023.10

**Perché:** violazione art. 5(1)(a), 5(1)(d), 5(2), 24 GDPR

**Come:** multa €75,000 + provvedimento

**Perché:** несколько граждан пожаловались на то, что получали от контролера множество нежелательных текстовых сообщений и, в одном случае, повторяющиеся рекламные телефонные звонки в течение шести лет, даже после того, как они выступили против этих сообщений.

Garante отметил, что даже после начала расследования со стороны Гаранта контролер уклонялся от сотрудничества в любой форме и не ответил ни на один запрос, направленный самим Гарантом. Таким образом, контролер нарушил законодательство о защите данных своим низким уровнем сотрудничества с Гарантом.

Кроме того, Garante предписал контролер установить соответствующие сроки хранения персональных данных, дать конкретные инструкции персоналу, чтобы запросы субъектов данных оперативно удовлетворялись, а также проверить технические и организационные меры, принятые для подтверждения получения действительного согласия на обработку данных в рекламных целях. Компании Università e-Campus было запрещено использовать персональные данные, обработанные незаконно.

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9939507>

# 964 Штраф за многочисленные нарушения GDPR



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Groupe Canal+

**Когда:** 2023.10

**За что:** нарушение ст. 7(1), 12, 13, 14, 15, 28, 32, 33 GDPR

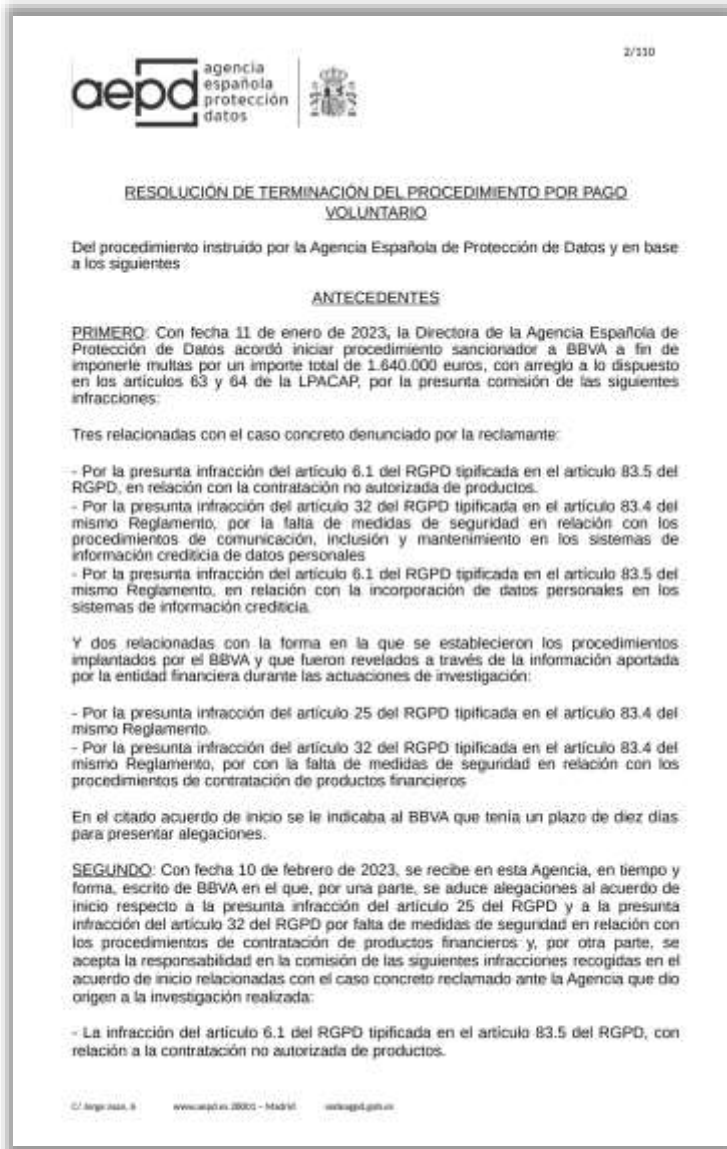
**Как:** штраф €600,000

**Причина:** контролер данных не смог доказать, что он получил действительно предварительное согласие от физических лиц на рассылку электронных рекламных сообщений. Кроме того, CNIL установил, что контролер данных не предоставил адекватной информации о сроках хранения персональных данных в своем заявлении о конфиденциальности.

Процессоры данных, привлеченные контролером, не предоставляли потенциальным клиентам достаточной информации во время маркетинговых звонков. В некоторых случаях контролер не отвечал должным образом на запросы субъектов данных. Контролер также не установил договорные правила обработки персональных данных со своими процессорами.

Наконец, контролер не обеспечил надлежащую защиту паролей сотрудников компании и не сообщил об утечке данных.

## Штраф за нереагирование на просьбу клиента заблокировать доступ к банковской учетной записи



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Banco Bilbao Vizcaya Argentaria, S.A. (BBVA)

**Когда:** 2023.10

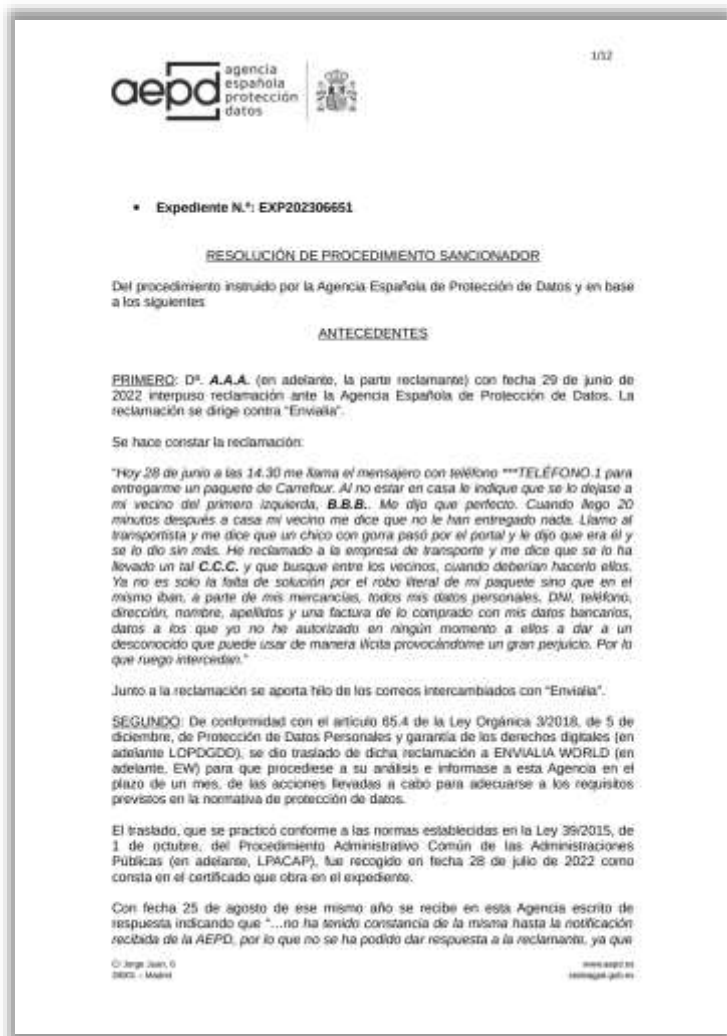
**За что:** нарушение ст. 25, 32(1) GDPR

**Как:** штраф €1,000,000

**Причина:** заявительница, являющаяся клиентом BBVA, потеряла кошелек, в котором среди прочих личных вещей находилась ее банковская карта. Заявительница обратилась в BBVA с просьбой заблокировать все её банковские транзакции. BBVA не выполнила просьбу заявительницы, и в последующие недели третьи лица, используя ранее скомпрометированные персональные данные, получили доступ к банковской учетной записи заявительницы, брали кредиты и переводили деньги с банковских счетов заявительницы.

Таким образом, что BBVA нарушил ст.32 GDPR, поскольку не принял надлежащих мер безопасности, что привело к краже персональных данных заявителя. Кроме того, BBVA нарушил ст.25 GDPR, не реализовав в своих банковских процессах принцип проектируемой защиты персональных данных.

## 966 Штраф за неправильно врученную посылку



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** The Bee Logistics SLU

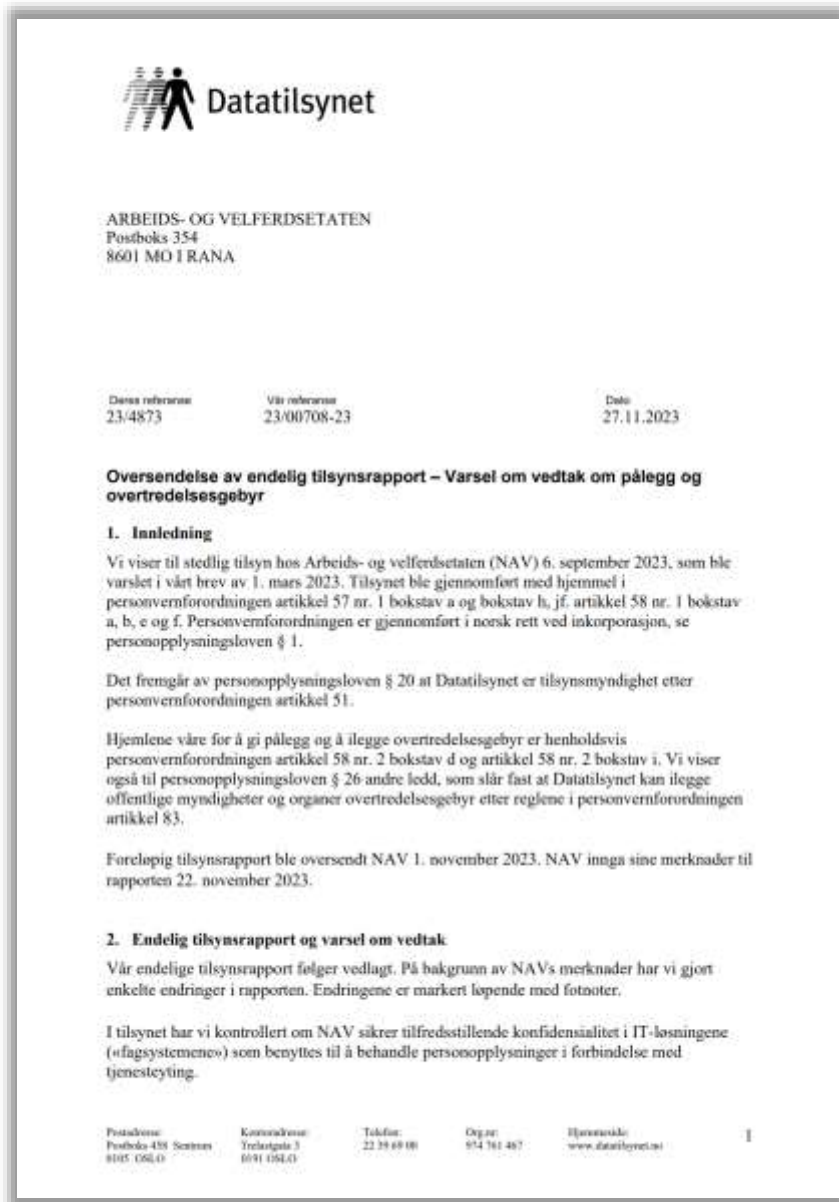
**Когда:** 2023.11

**За что:** нарушение ст. 5(1)(f), 32(1) GDPR

**Как:** штраф €70,000

**Причина:** заявительница должна была получить посылку от компании The Bee Logistics, которая выступала в качестве агентства по доставке Enviaia World S.L. Посылка вместо адресата была вручена другому лицу. Соответственно, персональные данные заявителя, включая имя, фамилию и почтовый адрес, были неправомерно раскрыты третьей стороне без согласия заявителя.

## Штраф за неэффективные технические и организационные меры защиты данных



**Кто:** Datatilsynet (Норвегия)

**Кого:** Arbeids- og velferdsetaten (Норвежское управление труда и социального обеспечения - NAV)

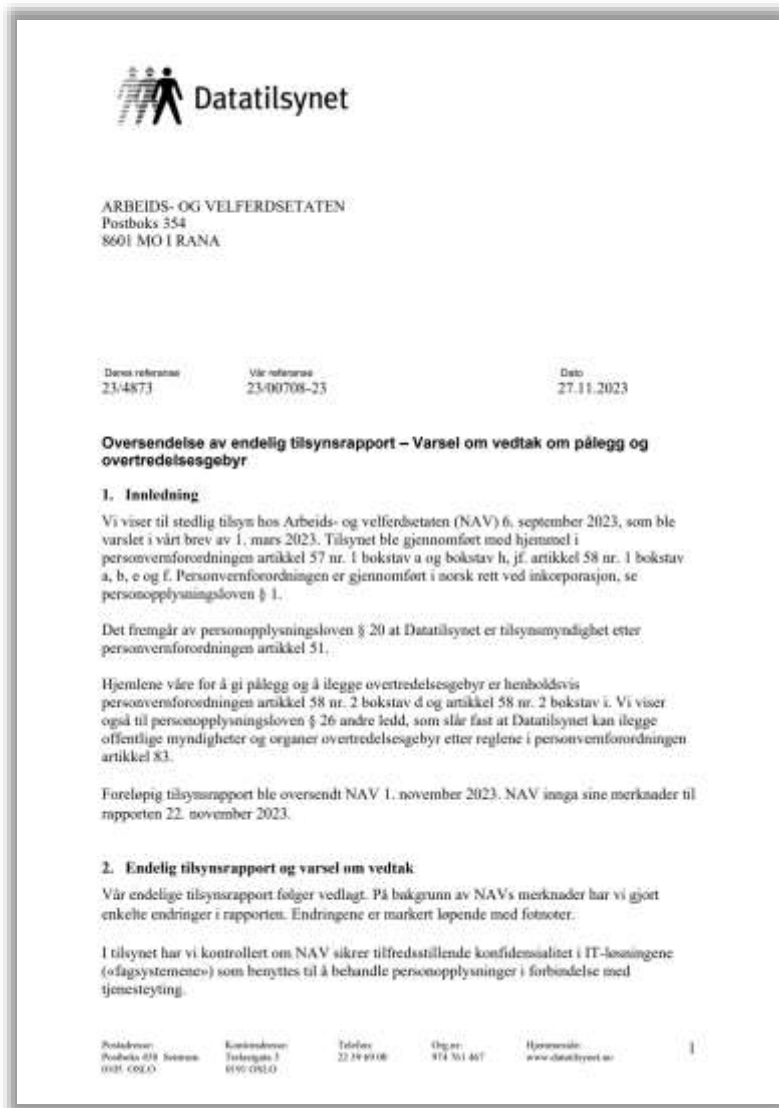
**Когда:** 2023.11

**За что:** нарушение ст. 5(1)(f), 5(2), 24(1), 25(1), 32(1)(d), 32(2) GDPR

**Как:** возможный штраф €1,700,000

**Причина:** в ходе расследования установлено, что контролер не принял надлежащих технических и организационных мер для защиты персональных данных. Например, ИТ-системы не были должным образом защищены. Кроме того, чрезмерное количество сотрудников имело доступ к персональным данным, в том числе в некоторых случаях очень чувствительным. В то же время контролер не осуществлял систематического контроля за использованием сотрудниками ИТ-систем. При определении размера штрафа надзорный орган принял во внимание тот факт, что данные небезопасно обрабатывались в течение длительного периода времени.

## 968 Штраф за непроведение DPIA перед началом использования Google Workspace



**Кто:** Integritetsskyddsmyndigheten (Швеция)

**Кого:** Департамент по делам детей и образования муниципалитета Эстерсунда (Östersund)

**Когда:** 2023.11

**За что:** нарушение ст. 35(1) GDPR

**Как:** штраф €26,500

**Причина:** в 2020 году Совет по делам детей и образования муниципалитета Эстерсунд (контролер) решил интегрировать Google Workspace в свои системы и школы, но не стал проводить оценку воздействия (DPIA), посчитав, что оценки 2014 года было достаточно. Только после такой интеграции контролер приступил к оценке воздействия. Этот процесс продолжался в течение трех лет и к моменту расследования надзорного органа так и не был завершен.



## Штраф за утечку данных, создавшую угрозу жизни сотрудничавшим с британскими властями афганцам



The screenshot shows the Information Commissioner's Office (ICO) website. The header includes the ICO logo and the tagline "The ICO exists to empower you through information." Below the header is a navigation menu with links: Home, For the public, For organisations, Make a complaint, and Action we've taken. The main content area features a news article titled "ICO fines Ministry of Defence for Afghan evacuation data breach" dated 13 December 2023. The article text states that the ICO has fined the Ministry of Defence (MoD) £350,000 for disclosing personal information of people seeking relocation to the UK shortly after the Taliban took control of Afghanistan in 2021. It details that an email sent to a distribution list of Afghan nationals eligible for evacuation had personal information, including email addresses and thumbnail pictures, inadvertently disclosed to 245 recipients. Two people replied to the entire list, with one providing their location. The article concludes that the original email, sent by the team in charge of the UK's Afghan Relocations and Assistance Policy (ARAP), should have fallen into the hands of the Taliban, potentially resulting in a threat to life.

**Кто:** Information Commissioner's Office (Великобритания)

**Кого:** министерство обороны Великобритании

**Когда:** 2023.12

**За что:** нарушение ст.32 UK GDPR

**Как:** штраф £350,000

**Причина:** В августе 2021 года власть в Афганистане захватили талибы, а представители западной коалиции бежали. Затем талибы начали поиск граждан, которые сотрудничали или работали на западные правительства. Пойманным грозила смерть.

В сентябре 2021 британские власти направили письма своим афганским сотрудникам, которым разрешалось эвакуироваться из страны. В копию письма были включены 245 получателей. Таким образом власти Великобритании по халатности раскрыли персональные данные своих агентов. Собственное расследование министерства обороны королевства выявило ещё ряд аналогичных случаев.

## 970 Штраф за использование Google Workspace for Education в начальной школе



**Úttekt á notkun Reykjanesbæjar á skýjalausn Google í grunnskólastarfi**

Mál nr. 2022020416  
6.12.2023

*Persónuupplýsingar barna njóta sérstakrar verndar. Þegar nota á upplýsingatækni kerfi í grunnskólastarfi er mikilvægt að hugað sé að þeirri vernd og farið að kröfum persónuverndarlöggjafarinnar til hins ýtrasta.*

*Í þessu máli notuðu grunnskólar Reykjanesbæjar upplýsingatækni kerfi án þess að gætt væri að kröfum persónuverndarlöggjafarinnar. Úttekt Persónuverndar á notkun kerfisins leiddi í ljós margvísleg brot sveitarfélagsins á löggjöfinni.*

—

Persónuvernd hefur lagt fyrir Reykjanesbæ að færa vinnslu persónuupplýsinga grunnskólanemenda í nemendakerfi Google, Google Workspace for Education, til samræmis við persónuverndarlöggjöfina. Að auki hefur 2.500.000 króna stjórnvaldssekt verið lögð á Reykjanesbæ.

Úttektin var ein af fimm úttektum sem Persónuvernd gerði á notkun skýjaþjónustu í grunnskólastarfi hjá stærri sveitarfélögum landsins. Voru þær þáttur í viðtækara verkefni sem unnið var að frumkvæði Evrópska persónuverndarráðsins. Úttektir Persónuverndar lutu að því hvernig persónuupplýsingar grunnskólanemenda sveitarfélaganna voru unnar í Google-nemendakerfinu. Leiddu úttektirnar í ljós að Google vinnur persónuupplýsingar grunnskólanemenda umfram fyrirmæli sveitarfélaganna og þótti ekki sýnt fram á að sú vinnsla rúmaðist innan þess tilgangs sem sveitarfélagin hafa skilgreint fyrir vinnslu persónuupplýsinga í nemendakerfinu.

**Кто:** Persónuvernd (Исландия)

**Кого:** пять муниципалитетов Исландии

**Когда:** 2023.12

**За что:** нарушение ст. 5(1), 24(1), 28 GDPR

**Как:** штраф на каждый муниципалитет €13,300-20,000

**Причина:** муниципалитеты использовали систему Google Education без достаточного соблюдения правил защиты данных. В частности, они не выполнили свои обязательства при выборе Google в качестве обработчика, а соглашение об обработке с Google не соответствовало требованиям GDPR.

Муниципалитеты допустили обработку данных учащихся в целях, отличных от тех, которые были указаны муниципалитетом. Срок хранения данных был признан излишне большим. Несмотря на отсутствие очевидного ущерба, было высказано мнение, что в прошлом использование Google Education создало угрозу безопасности данных при их передаче в США.

<https://www.personuvernd.is/urlausnir/utitekt-a-notkun-kopavogsbaejar-a-skyjalausn-google-i-grunnskolastarfi>  
<https://www.personuvernd.is/urlausnir/utitekt-a-notkun-hafnarfjardarbaejar-a-skyjalausn-google-i-grunnskolastarfi>  
<https://www.personuvernd.is/urlausnir/utitekt-a-notkun-gardabaejar-a-skyjalausn-google-i-grunnskolastarfi>  
<https://www.personuvernd.is/urlausnir/utitekt-a-notkun-reykjavikurborgar-a-skyjalausn-google-i-grunnskolastarfi>  
<https://www.personuvernd.is/urlausnir/utitekt-a-notkun-reykjanesbaejar-a-skyjalausn-google-i-grunnskolastarfi>

## 971 Штраф за утрату генетических данных



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Azienda Asl N.8 Di Cagliari

**Когда:** 2023.12

**За что:** нарушение ст. 5(1)(f), 5(2), 9, 32 GDPR

**Как:** штраф €18,000

**Причина:** субъект данных подал жалобу в связи с утратой биологических данных генетического характера, содержащихся в гистологических слайдах, хранящихся в некоторых медицинских картах, и их незаконным уничтожением. По данным аутсорсинговой компании (SISAR), которая отвечала за передачу образцов из патологоанатомического отделения, образцы были правильно доставлены в отдел медицинской документации. Однако более конкретная информация о получателях в отделе медицинской документации отсутствовала.

Что касается уничтожения тех же образцов, то срок хранения биологических образцов составлял не менее 10 лет, после чего требовалось провести оценку, чтобы определить, можно или нельзя уничтожить образцы. В данном случае контролер предположительно не провел такую оценку, поскольку не принял во внимание текущие судебные разбирательства, в которых образцы служили доказательством.

## 972 Штраф за невыполнение запроса работников о доступе к их данным



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Autostrade per l'Italia S.p.A.

**Когда:** 2023.12

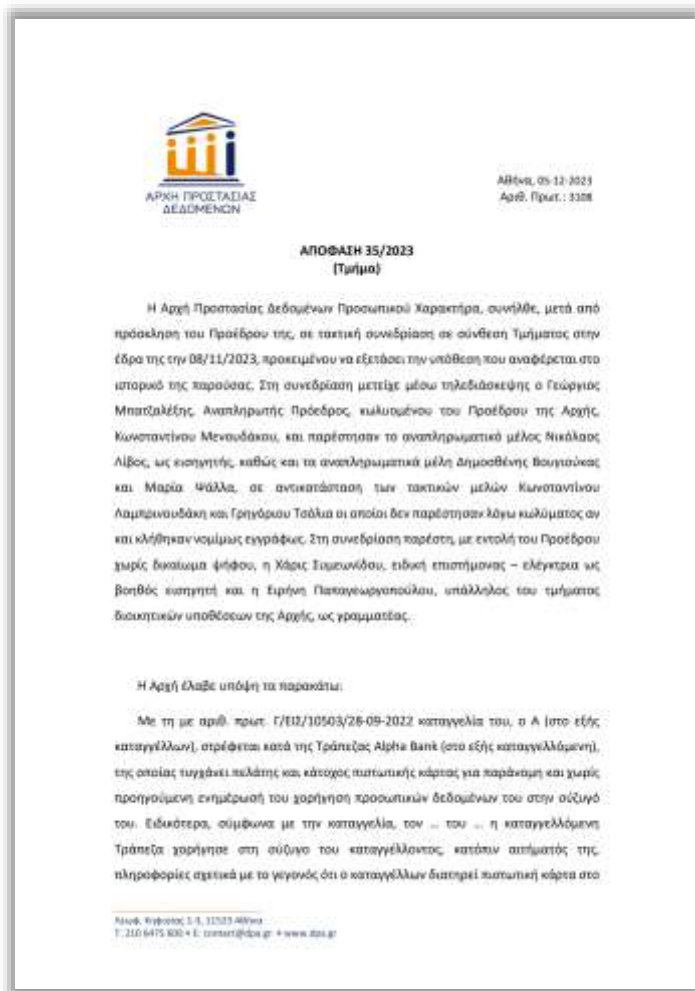
**За что:** нарушение ст. 12, 15 GDPR

**Как:** штраф €100,000

**Причина:** 50 сотрудников Autostrade запросили доступ к своим личным делам, расчетным листкам и ряду информации, касающейся обработки данных для расчета расчетных листков, не получив никакого ответа. Компания Autostrade не ответила на запрос работников, так как не сочла "целесообразным" отвечать на запрос, поскольку между Autostrade и ее работниками уже велось несколько судебных разбирательств по поводу предоставления и методов расчета выходного пособия.

Кроме того, Autostrade сообщила работникам только то, что они смогут узнать данные о своей зарплате, получив самостоятельный доступ к специальной IT-платформе. В нарушение статьи 12 GDPR Autostrade не предоставила работникам никакой обратной связи, чтобы сообщить о причинах невыполнения запросов, и не проинформировала о возможности подачи жалобы в надзорный орган и получения судебной защиты.

## Штраф за несанкционированное раскрытие персональных данных жене субъекта данных



**Κто:** Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

**Κого:** Alpha Bank

**Κогда:** 2023.12

**За что:** нарушение ст. 4(12), 5(1), 24(1), 33(1), 34(1) GDPR

**Как:** штраф €60,000

**Причина:** субъект данных (клиент банка) пожаловался на то, что Alpha Bank (контролер) предоставил жене заявителя информацию о ведении кредитной карты на его имя, а также распечатанные квитанции обо всех операциях, совершенных им за предыдущие 3-4 месяца, не уведомив его об этом. Это привело к значительному нарушению мира в семье и отношений заявителя с женой.

## Штраф за невыполнения требования об уничтожении данных и нарушение права на информированность



**Кто:** Nemzeti Adatvédelmi és Információszabadság Hatóság (Венгрия)

**Кого:** неназванная авиакомпания

**Когда:** 2023.12

**За что:** нарушение ст. 5(1)(а), 6(1), 12(3) и 17(1)(а) GDPR

**Как:** штраф €13,250

**Причина:** в октябре 2018 года клиент попросил авиакомпанию удалить все его персональные данные с сайта организации. Авиакомпания удалила учетную запись клиента через месяц, но не проинформировала об этом до марта 2019 года. При этом субъект данных не был проинформирован, какие дополнительные данные, с какой целью, на каком правовом основании и в течение какого времени обрабатывались оператором ПД после удаления учетной записи.

## 975 Штраф за нарушение правил хранения данных и сбора cookie-файлов



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** NS Cards France SAS

**Когда:** 2024.01

**За что:** нарушение ст. 5(1)(e), 12, 13, 32 GDPR

**Как:** штраф €105,000

**Причина:** компания NS Cards France, позволяющая пользователям совершать онлайн-платежи, требовала от пользователей создания учетной записи, чтобы совершать онлайн-платежи или получать выигрыши по купонам. При создании учетной записи собиралась личная информация, включая имя, дату рождения, адрес электронной почты, номер телефона, адрес электронной почты и банковские реквизиты, а также документы, удостоверяющие личность.

NS Cards France не обеспечивала надежную защиту паролей, разрешая использовать шестисимвольные пароли, состоящие только из символов нижнего и верхнего регистра, и не ограничивая доступ в случае неудачи при аутентификации. Кроме того, пароли хранились в открытом виде, при этом был виден и связанный с ними адрес электронной почты в качестве идентификатора.

Веб-сайт NS Cards France размещал 13 файлов cookie (включая файлы cookie для измерения аудитории от Google Analytics) на устройствах пользователей до того, как пользователь совершил какое-либо действие при переходе на веб-сайт.

## 976 Штраф за ненадлежащее проведение DPIA



**Who:** Autoriteit Persoonsgegevens (Нидерланды)

**Who:** Card Services B.V. (ICS)

**When:** 2024.01

**For what:** нарушение ст. 35 GDPR

**How:** штраф €150,000

**Reason:** ICS начала цифровую идентификацию клиентов в 2019 году, личная информация, используемая для идентификации, включала имена, адреса, номера телефонов, электронные адреса, а также фотографию, которую клиенты должны были сделать сами, и которая затем сравнивалась с идентификационными данными клиента. AP разъяснила, что финансовые учреждения обязаны идентифицировать своих клиентов.

Поскольку обрабатываемые персональные данные представляют высокий риск для прав и свобод физических лиц, ICS должна была провести оценку воздействия на защиту данных (DPIA). Проведенная ICS DPIA не обеспечивает систематического описания обработки, не позволяет оценить необходимость и пропорциональность обработки, а также меры, способствующие защите прав субъектов данных. Кроме того, неясно, участвовал ли в этой оценке DPO. В целом, ICS не признала, что речь идет о крупномасштабной обработке, тем самым нарушив GDPR.



## 977 Штраф за неадекватные меры безопасности



**DATATILSYNET**

Politianmeldelse

### Netcompany indstilles til bøde

Dato: 12-01-2024

Algoritmiske    Private virksomheder    Politianmeldelse    Anmeldt brud på persondataskikkerheden

Behandlingsikkerhed    Falsomme oplysninger    Risikovurdering og konsekvensanalyse

CPSR-nummer    Uautoriseret adgang

Datatilsynet politianmelder Netcompany og indstiller til en bøde på mindst 15 mio. kr. Ved udviklingen af mit.dk har virksomheden ikke sikret et passende sikkerhedsniveau, og der skulle have været udarbejdet en konsekvensanalyse, vurderer tilsynet.



Netcompany er blevet indstillet til en bøde på ikke under 15 mio. kr. for at have overtrådt databeskyttelsesforordningen i flere tilfælde, idet virksomheden som dataansvarlig ikke havde gennemført passende sikkerhedsforanstaltninger i forbindelse med udviklingen af mit.dk, herunder ikke sikret at der blev indbygget passende

**Кто:** Datatilsynet (Дания)

**Кого:** Netcompany (разработчик почтового сервиса mit.dk)

**Когда:** 2024.01

**За что:** нарушение ст. 25, 32, 35 GDPR

**Как:** штраф €2,012,000

**Причина:** компания не приняла надлежащих мер безопасности? Не реализовала принцип проектируемой приватности (privacy by design) и не провела DPIA при разработке цифрового почтового сервиса "mit.dk".

Netcompany узнала о ненадлежащем программном обеспечении почтового сервиса вскоре после запуска mit.dk, когда несколько пользователей обратились в компанию по поводу возможности доступа к информации других пользователей. После этого сервис был закрыто до тех пор, пока не был исправлен программный код, а о нарушении было сообщено в Datatilsynet.

## Штраф за использование «излишне интрузивной системы» мониторинга за деятельностью сотрудников на рабочем месте



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Amazon France Logistique

**Когда:** 2024.01

**За что:** нарушение ст. 5(1)(с), 6, 12, 32 GDPR

**Как:** штраф €32,000,000

**Причина:** каждому сотруднику французского подразделения Amazon выдаётся сканер [штрих-кодов] для «документирования процесса выполнения определённых задач, поставленных перед работником, в реальном времени».

При каждом сканировании, а для работников склада это постоянно выполняемая операция, происходит запись данных. Они хранятся и используются для определения качества и производительности труда персонала, а также для учёта времени, когда сотрудники не работают.

CNIL считает, что задействовать систему, точно фиксирующую каждый временной промежуток, в который работник не выполняет свои функции, незаконно. Требование компании сканировать предметы не дольше 1,25 секунды повышает риск ошибок. Кроме того, регулятор посчитал, что практика хранения Amazon всех собранных таким образом данных в течение 31 дня «избыточна».

Штраф также выписан за использование системы видеонаблюдения без необходимого информирования об этом и без обеспечения должного уровня безопасности.

## 979 Штраф за неназначение DPO



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Коммуна/муниципалитет Коуру (Commune de Kourou)

**Когда:** 2024.01

**За что:** нарушение ст. 31, 37(1)(a) GDPR

**Как:** штраф €5,000 + штраф в €150 за каждый день задержки исполнения предписания через 2 месяца после его получения + предписание опубликовать на сайте муниципалитета решение о назначении DPO

**Причина:** CNIL 02.06.2021 сообщила муниципалитету, что он не назначил DPO. Муниципалитет не ответил, поэтому 25.04.2022 CNIL направил муниципалитету официальное уведомление о необходимости назначить DPO в течение 4 месяцев после этого уведомления. Муниципалитет не ответил и на уведомление.

## Штраф за безосновательную опору на законный интерес при получении данных от третьих лиц и за другие нарушения



**Кто:** l'Autorité de protection des données (Бельгия)

**Кого:** Black Tiger Belgium


**Когда:** 2024.01

**За что:** нарушение ст. 5(1)(c), 5(1)(e), 6(1)(f), 12, 14, 15(1)(c), 15(1)(g), 15(3), 24(1), 25, 30(1)(c) GDPR

**Как:** штраф €174,640

**Причина:** контролер, являясь брокером данных, обработал большое количество персональных данных без ведома и предварительного согласия субъектов данных. Большое количество данных было отправлено различным сторонам и перепродано третьим лицам в коммерческих целях. Некоторые из персональных данных были получены более 15 лет назад и, следовательно, устарели. Кроме того, контролер применил к персональным данным профилирование, прежде чем продать их.

## Штраф за использование рекламных cookie без предварительного согласия и без учета отзыва согласия

 **Légifrance**  
 RÉPUBLIQUE FRANÇAISE  
 Liberté Égalité Fraternité

**Délibération SAN-2023-024 du 29 décembre 2023**

**Commission Nationale de l'Informatique et des Libertés**

Nature de la délibération : Sanction Date de publication sur Légifrance : Jeudi 18 janvier 2024  
 État juridique : En vigueur

**Délibération de la formation restreinte n°SAN-2023-024 du 29 décembre 2023 concernant la société YAHOO EMEA LIMITED**

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Alexandre LINDEN, président, M. Philippe-Pierre CABOURDIN, vice-président, MM. Alain DRU et Bertrand du MARAIS, membres ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données (RGPD) ;

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n°2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2020-127C du 14 août 2020 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à la vérification de la conformité à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 des traitements accessibles à partir du domaine "yahoo.com" ;

Vu les décisions n° 2020-254C du 14 août 2020 et n° 2021-123C du 4 janvier 2021 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par les sociétés VERIZON France et OATH BRANDS (France) SAS ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 19 juillet 2023 ;

Vu le rapport de M. François PELLEGRINI, commissaire-rapporteur, notifié à la société YAHOO EMEA LIMITED le 11 août 2023 ;

Vu les observations écrites versées par la société YAHOO EMEA LIMITED le 29 septembre 2023 ;

Vu la réponse du rapporteur à ces observations notifiée à la société YAHOO EMEA LIMITED le 25 octobre 2023 ;

Vu les nouvelles observations écrites versées par la société YAHOO EMEA LIMITED le 28 novembre 2023 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 21 décembre 2023 ;

Vu les autres pièces du dossier ;

[https://www.legifrance.gouv.fr/consulter/CNILTEXT000048967251?page=1&pageSize=10&query=2016%252F679&searchField=ALL&searchType=ALL&sortValue=DATE\\_DECISION\\_DESC&tab\\_selection=cnil&typePagination=DEFAULT](https://www.legifrance.gouv.fr/consulter/CNILTEXT000048967251?page=1&pageSize=10&query=2016%252F679&searchField=ALL&searchType=ALL&sortValue=DATE_DECISION_DESC&tab_selection=cnil&typePagination=DEFAULT) 1/16

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Yahoo EMEA Limited

**Когда:** 2024.01

**За что:** нарушение ст. 6(1), 7(3), 7(4) GDPR

**Как:** штраф €10,000,000

**Причина:** CNIL провела онлайн-расследование на сайте "yahoo.com" и в службе обмена сообщениями "Yahoo mail". Было обнаружено, что на терминале пользователя было размещено не менее 20 файлов cookie для рекламных целей, хотя он не давал на это согласия. На странице Yahoo было окно "Ваши данные. Ваш опыт", в котором были кнопки "Я принимаю" и "Управление настройками". Кнопка "Управление настройками" использовала кнопки, которые были активированы по умолчанию. CNIL не активировал ни одну из кнопок и нажал "Сохранить и продолжить", но при этом отметил размещение 26 файлов cookie, 7 из которых использовались в рекламных целях.

## Штраф за использование систем наблюдения на основе искусственного интеллекта для научных исследований



**Chi:** Garante per la protezione dei dati personali (Italia)

**Chi:** Comune di Trento (municipalitet Trento)

**Quando:** 2024.01

**Per che:** нарушение ст. 5(1)(a), 6, 9, 10, 13, 14, 35 GDPR

**Как:** штраф €50,000

**Причина:** в рамках социального эксперимента муниципалитет Trento (контролер) разрешил развернуть три проекта, "Marvel" и "Protector", которые уже завершены, и "Precrisis", который еще предстоит активировать, используя системы искусственного интеллекта (ИИ), разработанные исследовательского фонда FBK, для сбора данных в общественных местах муниципалитета с помощью видеокамер и микрофонов, которые могли бы служить цели предотвращения потенциальных ситуаций, представляющих опасность для населения.

Хотя проекты были экспериментальными и данные не использовались в целях предотвращения преступлений, контролер все равно осуществлял обработку персональных данных, связанных с уголовным осуждением и правонарушениями. Контролер заявил, что он применил методы анонимизации сразу после сбора данных: изменение звука голоса в голосовых записях и размытие лиц людей в видеозаписях. Garante считал эти методы недостаточными, поскольку они не гарантировали полной анонимизации собранных персональных данных. Собранные на платформах социальных сетей данные были просто псевдонимизированы, а не анонимизированы, как утверждал контролер.

## 983 Штраф за несообщение контактных данных DPO



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Comune di Syracuse (муниципалитет Сиракуз)

**Когда:** 2024.02

**За что:** нарушение ст. 37(7) GDPR

**Как:** штраф €5,000

**Причина:** в рамках инициативы, направленной на содействие выполнению обязательств по защите персональных данных, муниципалитет Сиракуз был уведомлен о том, что контактные данные назначенного лица по защите данных (DPO) не были представлены Garante должным образом. Дополнительная проверка на веб-сайте муниципалитета Сиракуз выявили публикацию контактных данных DPO.

## 984 Штраф за недостаточную прозрачность в политике конфиденциальности

**Кто:** Autoriteit Persoonsgegevens (Нидерланды)

**Кого:** Uber Technologies Inc. и Uber B.V. (совместные контролеры)

**Когда:** 2024.02

**За что:** нарушение ст. 12, 13 и 15 GDPR

**Как:** штраф €10,000,000

**Причина:** французская правозащитная организация Ligue des droits de l'Homme (LDH) подала жалобу от имени 172 водителей Uber против Uber B.V. и ее американской материнской компании Uber Technologies Inc. как совместных контролеров.

В политике конфиденциальности Uber указана слишком общая информация о сроках хранения данных, которые будут храниться "столько, сколько необходимо". Также не были указаны третьи страны, в которые могут быть переданы персональные данные, а также действующие гарантии и место доступа к ним. Политика также не содержала никакого упоминания о возможности субъектам воспользоваться своим правом на перенос данных.

Форма для направления запросов субъектов данных, доступная в приложении Uber, не является достаточно легкодоступной, поскольку она включает в себя слишком много неинтуитивных шагов. В таких формах можно использовать многоуровневую структуру информации, но при этом необходимо соблюдать баланс между количеством шагов, которые нужно пройти, и объемом информации, включенной в каждый шаг, а кроме того, шаги должны иметь понятные и интуитивно понятные названия.

Uber предоставляет информацию в CSV-файле в ответ на запросы субъектов о доступе к данным, не добавляя никаких указаний о том, как информация из такого файла может быть структурирована и интерпретирована. После добавления руководства о том, как открыть и прочитать CSV-файлы, Uber предоставила такую информацию только на английском языке, хотя Uber предлагает услуги во многих странах ЕС, что негативно сказывается практически на всех водителях Uber в Европе.



## 985 Штраф за незаконный сбор биометрии клиентов



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Metropolitan Spain S.L.

**Когда:** 2024.02

**За что:** нарушение ст. 6(1), 9(1), 13 GDPR

**Как:** штраф €27,000

**Причина:** Заявитель был клиентом тренажерного зала, которым управляет Metropolitan Spain. До мая 2021 года он проходил в зал с помощью браслета и документами, удостоверяющими личность. Но позднее доступ стал возможен только при сканировании отпечатков пальцев. После отказа предоставить данные об отпечатках клиенту сообщили, что его членство в зале будет прекращено.


Регистрация отпечатков пальцев для доступа в зал не была необходимой для исполнения контракта, поскольку в прошлом заявитель использовал другие средства доступа. Поэтому Metropolitan Spain не имела законных оснований для обработки данных.

Обработка биометрических дан не подпадает ни под одно из исключений, предусмотренных ст.9(2) GDPR. Metropolitan Spain не проинформировала заявителя о последствиях непредоставления сведений об отпечатках пальцев во время сбора данных.



## 987 Штраф за нарушение безопасности данных клиентов

40214

 **agencia española protección datos**

Adopción de medidas:.....217  
la Directora de la Agencia Española de Protección de Datos RESUELVE:.....217

**ANTECEDENTES**

**PRIMERO:** Con fecha 10 de febrero de 2022, se notificó a la Agencia Española de Protección de Datos (AEPD) una violación de seguridad de los datos personales, remitida por ENDESA ENERGÍA, S.A.U. con NIF A81948077 (en adelante, ENDESA), consistente en un posible acceso no autorizado a ciertos sistemas comerciales de Endesa Energía que podría haber afectado a unos mil clientes.

En esta notificación se informa a la AEPD de lo siguiente:

En agosto de 2021, se detectan ciertos anuncios de Facebook que anuncian la venta de credenciales para acceder a la plataforma **\*\*\*PLATAFORMA.1** de ENDESA (que contiene datos básicos y relativos al punto de suministro). Se valoró ese incidente y se adoptaron las medidas pertinentes. El 17/01/2022 se detecta un anuncio de Facebook con características similares a los anteriores que informa de la venta de bases de datos de clientes de energía y gas. Se hace una valoración del anuncio y no se encuentran coincidencias con datos de clientes de ENDESA incluidos en el sistema CRM. El 02/02/2022 se detectan datos de, entre otros, algunos clientes de ENDESA incluidos en el sistema CRM.

Número aproximado de personas físicas sobre las que recoge, almacena o trata datos personales de otra forma, referido exclusivamente al tratamiento sobre el que se ha producido la brecha de datos personales: 6.500.000.

El incidente ha sido: Intencionado, para hacer daño al responsable / encargado o a las personas afectadas.

El origen del incidente ha sido: Externo; Otros, ajenos al responsable y encargado del tratamiento

¿Qué puede haber ocurrido?: Abuso de privilegios de acceso por parte de empleado para extraer, reenviar o copiar datos personales

Como consecuencia del incidente, se ha visto afectada la: Confidencialidad

Referido específicamente a los datos afectados por la brecha de confidencialidad. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso o no se puede identificar a las personas?: No

¿Qué puede haber ocurrido?: Usurpación de identidad. Pérdida de control sobre sus datos personales.

¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas?:

© Jorge Juan, S.  
2021 - Madrid

www.aepd.es  
resolución 40214

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Endesa Energía, S.A.U.

**Когда:** 2024.02

**За что:** нарушение ст. 32-34, 44 GDPR

**Как:** штраф €6,100,000

**Причина:** AEPD заявила, что получила уведомление о нарушении безопасности персональных данных, направленное компанией Endesa и заключающееся в возможном несанкционированном доступе к некоторым коммерческим системам Endesa, который мог затронуть около тысячи клиентов. Кроме того, в августе 2021 года были обнаружены объявления в Facebook о продаже учетных данных для доступа к платформе Endesa, которые содержали основные данные, связанные с точкой поставки.

## Штраф за нарушения при обработке сведений о сексуальной ориентации и сексуальных предпочтениях



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Nirvam S.r.l. (сайт онлайн-знакомств)

**Когда:** 2024.02

**За что:** нарушение ст. 5, 7, 9, 13, 30, 32, 35 и 37 GDPR

**Как:** штраф €200,000

**Причина:** Nirvam обрабатывает информацию более чем 1 млн зарегистрированных пользователей, часто содержащуюся в фотографиях, которые загружаются в публичный профиль пользователя. Обработка касается чувствительных категорий данных, включая сексуальную ориентацию и сексуальные предпочтения.

Nirvam не имела специальной политики, касающейся сроков хранения персональных данных. Также отсутствовали надлежащие технические и организационные меры защиты данных.

Обработка сведений о сексуальной ориентацией и сексуальными предпочтениями должна осуществляться только с явного согласия субъекта, а получения явного и информированного согласия не предусмотрена.

Nirvam не вела учет деятельности по обработке данных (ROPA), не назначила ответственного за защиту данных (DPO), не провела оценку воздействия на частную жизнь (DPIA) и не установила системы обнаружения вторжений в ИТ-системы и процедуру аварийного восстановления данных.

## Штраф за незаконную маркетинговую деятельность и покупку баз данных контактов



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** Enel Energia S.p.A. (Enel Energia)

**Когда:** 2024.02

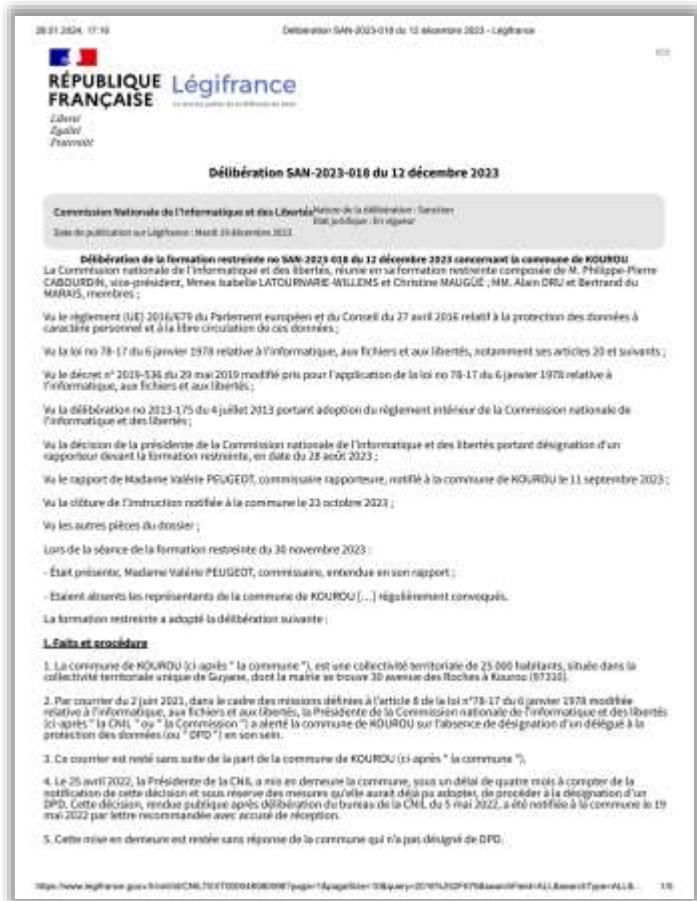
**За что:** нарушение ст. 5(1)(f), 5(2), 24(1), 25, 32 GDPR

**Как:** штраф €79,100,000

**Причина:** финансовая полиция (Guardia di Finanza) провела расследование, в ходе которого были наложены штрафы на четыре компании и конфискованы базы данных, поскольку они имели отношение к незаконной деятельности.

Дальнейшее изучение баз данных показало, что Enel Energia приобрела 978 контрактов у четырех компаний, хотя эти компании не входили в сбытовую сеть Enel Energia. Дополнительное расследование показало, что маркетинговая деятельность Enel Energia осуществлялась с использованием незаконно приобретенных списков клиентов, содержащих адреса, номера телефонов, муниципалитеты проживания клиентов, а также соответствующую энергетическую компанию клиента.

## 990 Штраф за неправомерное хранение и ненадлежащую защиту данных



**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** De Particulier A Particulier (PAP)

**Когда:** 2024.02


**За что:** нарушение ст. 5(1)(e), 13, 28(3), 32 GDPR

**Как:** штраф €100,000

**Причина:** компания PAP ввела 10-летний срок хранения данных о счетах некоторых клиентов с момента принятия заказа. Период хранения был систематическим и неизбирательным, относящимся в некоторых случаях к транзакциям на сумму менее 120 евро. Примечательно, что PAP также установила срок хранения данных в пять лет с момента последнего подключения к аккаунту для бесплатных пользователей сайта PAP, однако на практике такой срок не применялся. Сохраняемые данные включали имена и фамилии, номера телефонов и адреса электронной почты клиентов. Соответственно, поскольку PAP сохраняла личные данные сверх установленного срока хранения и сверх того, что было необходимо для заявленной цели.

## 991 Штраф за передачу данных сотрудника через Whatsapp

40214

 **agencia española protección datos**

Adopción de medidas:.....217  
la Directora de la Agencia Española de Protección de Datos RESUELVE:.....217

**ANTECEDENTES**

**PRIMERO:** Con fecha 10 de febrero de 2022, se notificó a la Agencia Española de Protección de Datos (AEPD) una violación de seguridad de los datos personales, remitida por ENDESA ENERGÍA, S.A.U. con NIF A81948077 (en adelante, ENDESA), consistente en un posible acceso no autorizado a ciertos sistemas comerciales de Endesa Energía que podría haber afectado a unos mil clientes.

En esta notificación se informa a la AEPD de lo siguiente:

En agosto de 2021, se detectan ciertos anuncios de Facebook que anuncian la venta de credenciales para acceder a la plataforma **\*\*\*PLATAFORMA.1** de ENDESA (que contiene datos básicos y relativos al punto de suministro). Se valoró ese incidente y se adoptaron las medidas pertinentes. El 17/01/2022 se detecta un anuncio de Facebook con características similares a los anteriores que informa de la venta de bases de datos de clientes de energía y gas. Se hace una valoración del anuncio y no se encuentran coincidencias con datos de clientes de ENDESA incluidos en el sistema CRM. El 02/02/2022 se detectan datos de, entre otros, algunos clientes de ENDESA incluidos en el sistema CRM.

Número aproximado de personas físicas sobre las que recoge, almacena o trata datos personales de otra forma, referido exclusivamente al tratamiento sobre el que se ha producido la brecha de datos personales: 6.500.000.

El incidente ha sido: Intencionado, para hacer daño al responsable / encargado o a las personas afectadas.

El origen del incidente ha sido: Externo; Otros, ajenos al responsable y encargado del tratamiento

¿Qué puede haber ocurrido?: Abuso de privilegios de acceso por parte de empleado para extraer, reenviar o copiar datos personales

Como consecuencia del incidente, se ha visto afectada la: Confidencialidad

Referido específicamente a los datos afectados por la brecha de confidencialidad. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso o no se puede identificar a las personas?: No

¿Qué puede haber ocurrido?: Usurpación de identidad. Pérdida de control sobre sus datos personales.

¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas?:

© Jorge Juan, S.  
2021 - Madrid

www.aepd.es  
Resolución 00549/2022

**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** неназванная компания

**Когда:** 2024.02

**За что:** нарушение ст. 5(1)(f) GDPR

**Как:** штраф €5,000

**Причина:** субъект данных подал жалобу на своего работодателя (контролера). Он отправил контролеру служебное электронное письмо по трудовому вопросу. Затем контроллер отобразил скриншот этого письма в профиле субъекта данных в Whatsapp. На скриншоте были указаны имя и фамилия субъекта данных, а также вопрос о трудовом вопросе. Испанский надзорный орган несколько раз обращался к контроллеру за разъяснениями, но каждый раз был проигнорирован и не получил ответа.

## Штраф за распространение сведений о дефекте кожи на корпоративном аккаунте в Instagram

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** David S.r.l. (эстетический центр «Dvora»)

**Когда:** 2024.02

**За что:** нарушение ст. 5(1)(а), 6, 9, 12 и 13 GDPR

**Как:** штраф €8,000

**Причина:** субъект данных, который был снят на видео во время процедуры эстетической медицины в эстетическом центре «Dvora» пожаловался на незаконное распространение его персональных данных на аккаунте контролера в Instagram. В ответ на жалобу контролер представил доказательства того, что субъект данных дал конклюдентное («молчаливое») согласие на обработку и публикацию своих данных и изображений в социальных сетях. Однако субъект данных заявил, что не давал согласия на съемку видео, на котором его лицо было бы узнаваемо вместе с расширенными во время эстетической процедуры порами кожи, которые, по мнению субъекта, относятся к состоянию его здоровья.

Итальянский надзорный орган (Garante) пояснил, что чувствительный характер информации должен оцениваться также в зависимости от контекста упоминания. Несмотря на отсутствие явного указания на патологию, которой, возможно, страдает субъект данных, Garante расценил запись о недостатках лица субъекта данных как данные о здоровье, поскольку контролер утверждал, что проводит "безоперационную ринопластику" - процедуру, связанную с состоянием здоровья человека.

По этой причине конклюдентное согласие субъекта данных не может считаться действительным, поскольку обработка подпадает под исключения из запрета на обработку чувствительных категорий данных согласно ст.9(2)(а) GDPR при условии, что они могут обрабатываться только на основании явно выраженного согласия субъекта данных. Таким образом, даже если субъект данных был осведомлен о съемках медицинских услуг, которые он проходил, это обстоятельство не равнозначно получению от субъекта данных информированного, конкретного и явного согласия на то, как данные, подлежащие той же записи, будут обрабатываться и, в данном случае, даже распространяться на социальных платформах.



## 993 Штраф за нарушения при установлении сроков хранения данных

**Commission Nationale de l'Informatique et des Libertés**  
Nature de la délibération : Sanction Date de publication sur Légifrance : Jeudi 18 janvier 2024  
État juridique : En vigueur

**Délibération de la formation restreinte n°SAN-2023-024 du 29 décembre 2023 concernant la société YAHOO EMEA LIMITED**

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Alexandre LINDEN, président, M. Philippe-Pierre CABOURDIN, vice-président, MM. Alain DRU et Bertrand du MARAIS, membres ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données (RGPD) ;

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n°2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2020-127C du 14 août 2020 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à la vérification de la conformité à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 des traitements accessibles à partir du domaine "yahoo.com" ;

Vu les décisions n° 2020-254C du 14 août 2020 et n° 2021-123C du 4 janvier 2021 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par les sociétés VERIZON France et OATH BRANDS (France) SAS ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 10 juillet 2023 ;

Vu le rapport de M. François PELLEGRINI, commissaire-rapporteur, notifié à la société YAHOO EMEA LIMITED le 11 août 2023 ;

Vu les observations écrites versées par la société YAHOO EMEA LIMITED le 29 septembre 2023 ;

Vu la réponse du rapporteur à ces observations notifiée à la société YAHOO EMEA LIMITED le 25 octobre 2023 ;

Vu les nouvelles observations écrites versées par la société YAHOO EMEA LIMITED le 28 novembre 2023 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 21 décembre 2023 ;

Vu les autres pièces du dossier ;

<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000049128617?page=1&pageSize=10&query=2016%252F679&searchField=ALL&searchType=ALL...> 5/15

**Кто:** Commission nationale de l'informatique et des libertés (Франция)

**Кого:** Société Particulier à Particulier - Editions Neressis (Société PAP)

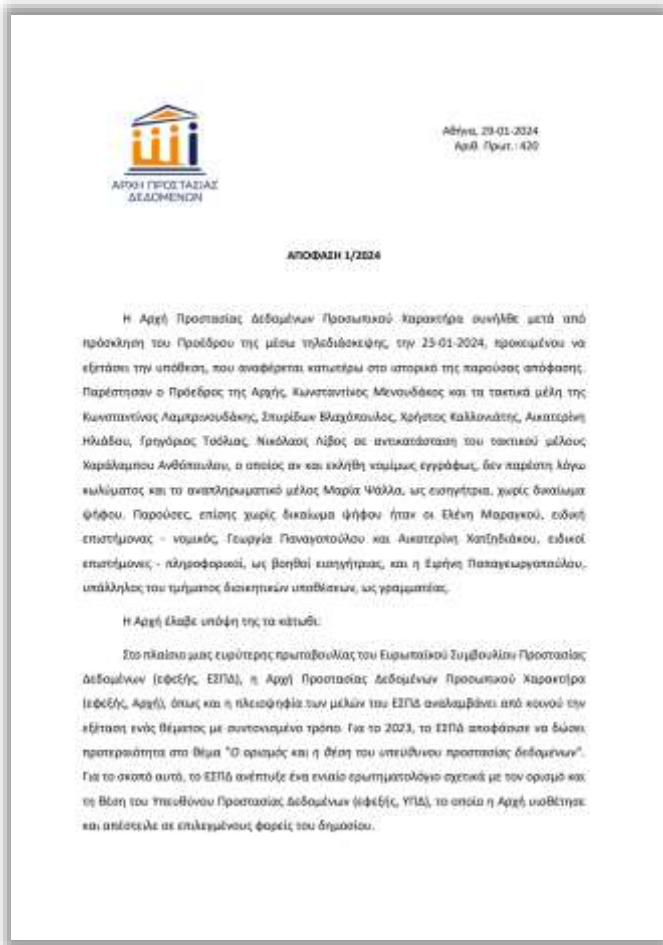
**Когда:** 2024.02

**За что:** нарушение ст. 5(1)(e), 13, 28, 32 GDPR

**Как:** штраф €100,000

**Причина:** контролер предоставляет частным лицам набор публикаций и услуг, позволяющих им заключать сделки с недвижимостью без посредников. Контролер определил срок хранения данных в десять лет с момента принятия заказа на сайте (в т.ч. для контрактов, заключенных в электронном виде, на сумму менее 120 евро.) и не включил в свою политику конфиденциальности право на подачу жалобы в надзорный орган, правовую основу для каждой обработки, а также получателей и категории получателей.

Также контролер определил 5-летний период хранения данных, начиная с даты последнего подключения к учетной записи пользователя, оправдан для целей судебного разбирательства и борьбы с мошенничеством, но было сохранено более 2 миллионов учетных записей пользователей возрастом от 5 до 10 лет, а также более 700,000 учетных записей возрастом более 10 лет.



**Κτο:** Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

**Κογο:** Δήμος Αθηναίων (муниципалитет Αφιν)

**Κοгда:** 2024.02

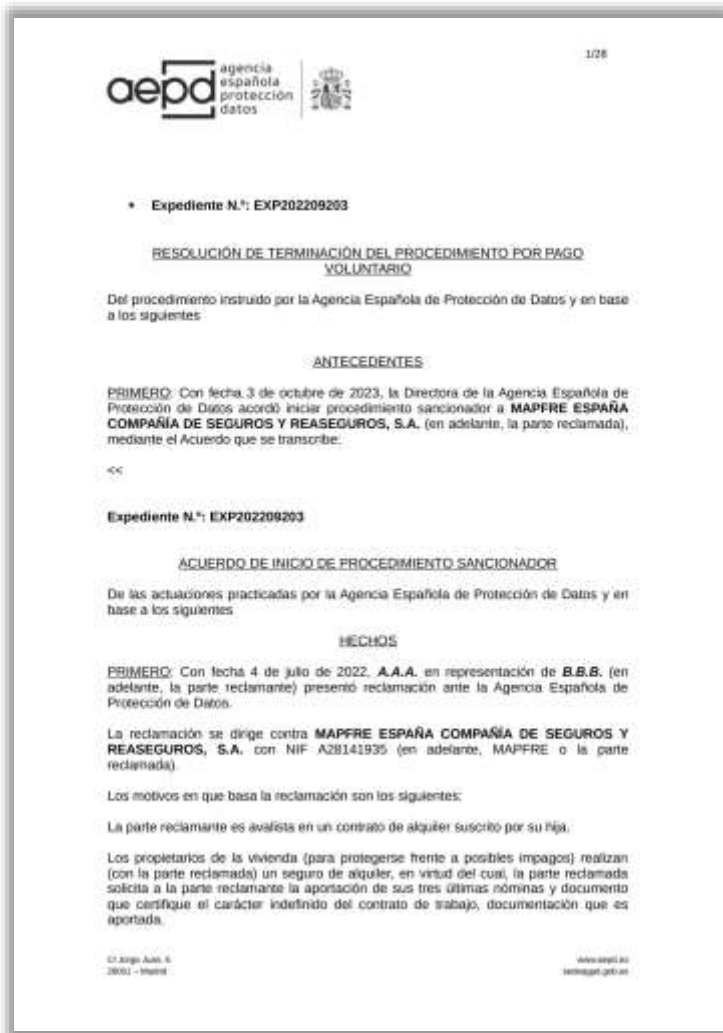
**За что:** нарушение ст. 31, 37, 38, 39 GDPR

**Как:** штраф €5,000

**Причина:** Греческое управление по защите данных (HDPA) в рамках изучения темы "Определение и должность DPO" направило ряду организаций унифицированную анкету. DPO муниципалитета Αφιν не ответил на анкету в установленный срок. HDPA повторно отправил анкету – и снова DPO не ответил. После истечения срока DPO попытался заполнить анкету, но безуспешно, поскольку вышеуказанная ссылка была деактивирована HDPA. После того как DPO связался с HDPA, ссылка была восстановлена, но DPO опять не представил анкету.

После этого HDPA вызвал контролера на дачу объяснений. DPO связался с HDPA по телефону и сообщил, что по ошибке не смог ответить на вопросник из-за технических проблем, и обязался заполнить и представить его немедленно. После этого DPA Греции вновь активировал ссылку на отправку анкеты, и DPO в итоге отправил анкету. Позже DPO еще раз заявил, что причиной задержки ответа стали технические проблемы с веб-сайтом, на котором размещалась анкета, которые не позволили отправить анкету даже после нескольких попыток.

## 995 Штраф за сбор избыточных данных у клиентов страховой компании



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Mapfre España

**Когда:** 2024.03

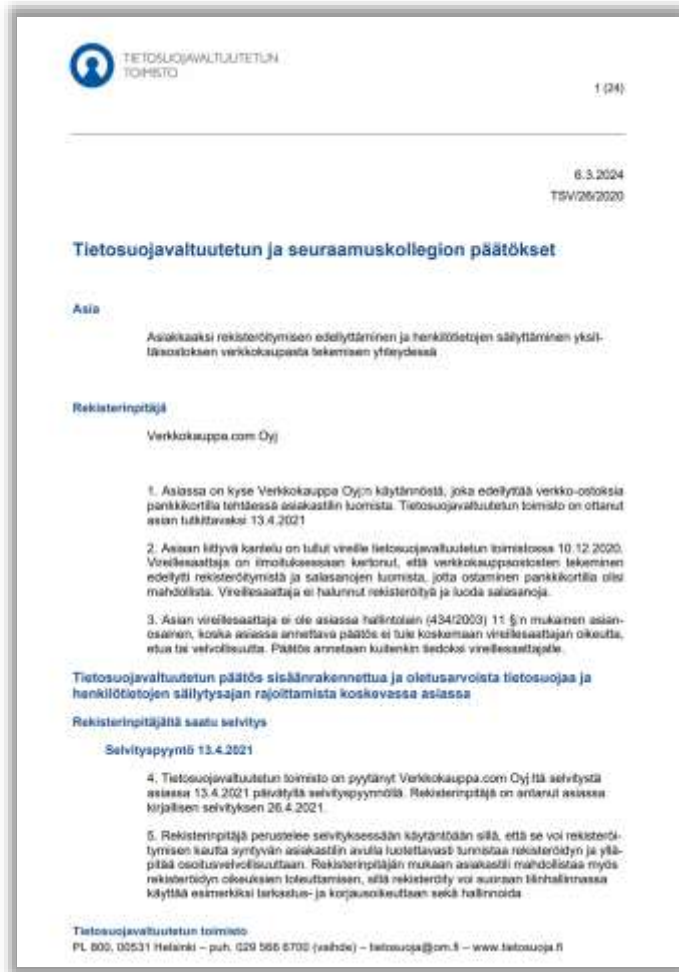
**За что:** нарушение ст. 5(1)(с) GDPR

**Как:** штраф €684,000

**Причина:** заявители утверждали, что для проверки платежеспособности страховая компания (контролер) просила их предоставить личную информацию, в том числе копии документов об уплате подоходного налога и информацию о трудовой биографии.

АEPD установила, что запрос дополнительной документации привело к нарушению принципа минимизации данных («Dataminimization»), который требует, чтобы сбор данных был адекватным, релевантным и необходимым в отношении целей обработки.

## Штраф за требование регистрации в интернет-магазине для совершения покупки товара



**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

**Кого:** Verkkokauppa.com Oy

**Когда:** 2024.03

**За что:** нарушение ст. 5(1), 6(1) GDPR

**Как:** штраф €856,000

**Причина:** клиент пожаловался на требование Verkkokauppa создать учетную запись перед совершением онлайн-покупки. Также интернет-магазин хранил информацию об учетной записи клиента в течение неопределенного периода времени, считает Ombudsman.

Для покупки в интернете не требуются персональные данные или создание учетной записи клиента, поэтому Verkkokauppa нарушила нормы GDPR.

Verkkokauppa должна определить срок хранения сведений об учетной записи клиента и скорректировать свои правила создания учетной записи.

## 997 Штраф за несвоевременное уведомление о результатах пентеста

**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** NTT DATA Italia S.p.A.

**Когда:** 2024.03

**За что:** нарушение ст. 28(2) и 33(2) GDPR

**Как:** штраф €800,000

**Причина:** 21.10.2018 произошла кибератака на систему мобильного онлайн-банкинга UniCredit S.p.A. (UniCredit), в результате которой произошла утечка персональных данных некоторых клиентов банка (имя, фамилия, налоговый код и внутренний идентификационный код банка за вычетом банковских реквизитов клиента). Компания NTT DATA Italia которая отвечала за проведение тестов на проникновение и оценку уязвимостей с 01.10.2018 по 26.10.2018 для UniCredit. В ходе расследования было установлено, что NTT DATA Italia заключила контракт с третьей компанией (субподрядчиком) на проведение пентеста для UniCredit от ее имени без надлежащего разрешения UniCredit.

Итальянский надзорный орган решил, что NTT DATA Italia поручила проведение оценки уязвимости и тестирования на проникновение портала мобильного банкинга сторонней компании в отсутствие предварительного письменного разрешения от контролера данных (в данном случае UniCredit) в нарушение ст.28(2) GDPR. Кроме того, NTT DATA Italia получила от своего субподрядчика отчет об оценке уязвимостей и результатах пентеста 19.10.2018 и проинформировала UniCredit о результатах 22.10.2018 года в нарушение ст.33(2) GDPR.

При этом сам банк UniCredit [был оштрафован](#) спустя 5,5 лет (!) после утечки данных на €2,800,000 за нарушение ст. 5(1)(f) и 32 GDPR

## Штраф за использовании поля "Кому" вместо поля "Слепая копия" при отправке электронных писем пользователям мобильного приложения



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** La società Medtronic Italia

**Когда:** 2024.03

**За что:** нарушение ст. 5(1)(a), 5(1)(f), 9, 12, 13, 32 GDPR

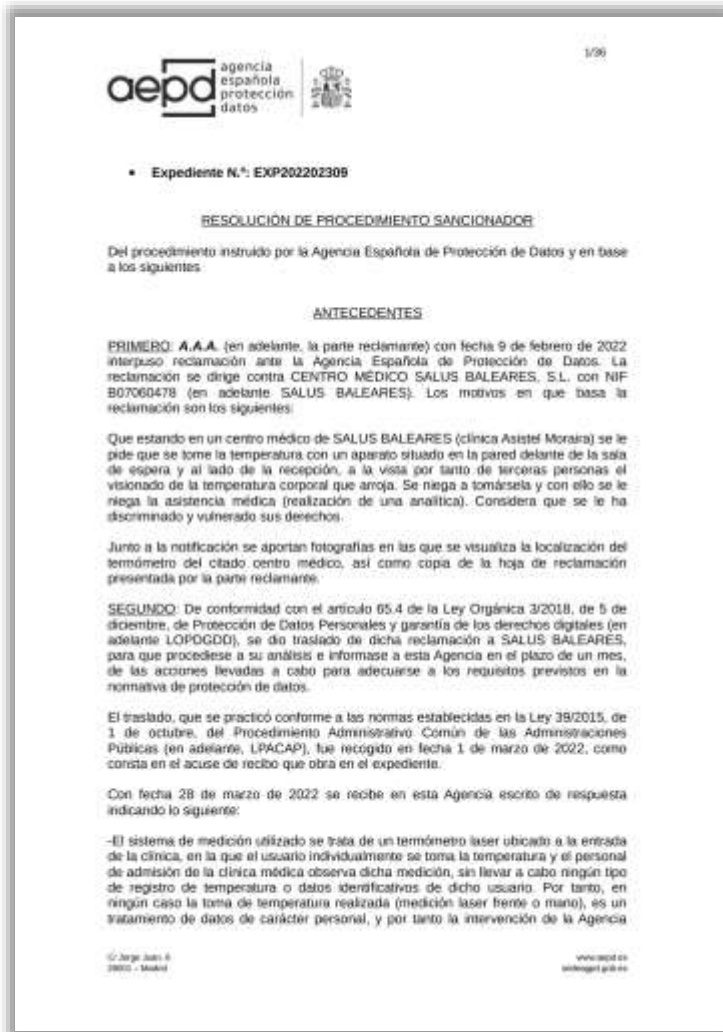
**Как:** штраф €300,000

**Причина:** приложение MiniMed Mobile отображает данные инсулиновой помпы и непрерывного мониторинга глюкозы, а также обеспечивает прямую связь с медицинским работником пациента через персональное программное обеспечение "CareLink".

Сотрудник владельца приложения отправил электронное письмо пользователям приложения MiniMed Mobile в разных странах ЕС и за его пределами, чтобы уведомить их об обновлении системы обслуживания сервера и о шагах, необходимых для восстановления доступа к персональному программному обеспечению "CareLink" в рамках этого обновления.

Адреса электронной почты получателей были внесены в поле "Кому" вместо поля "Слепая копия" (BCC). В результате были раскрыты около 5,000 адресов электронной почты пользователей приложения MiniMed Mobile по всему миру, включая 732 адреса в Италии.

## Штраф за уведомление сотрудников об использовании биометрических данных



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** CTC Externalización S.L. (CTC)

**Когда:** 2024.02

**За что:** нарушение ст. 13, 32, 35 GDPR

**Как:** штраф €365,000

**Причина:** CTC запросила отпечатки пальцев у сотрудников с целью внедрения системы регистрации на основе отпечатков пальцев, но во время снятия таких данных не было сообщено, что они хранятся на портале для сотрудников. Что касается реализации технических и организационных мер безопасности, CTC не доказала, как гарантируется стирание исходного отпечатка пальца сотрудника после создания на его основе биометрического вектора.

Наконец, не рассматривала обработку биометрических данных как обработку специальных категорий данных или риски для прав и свобод сотрудников и не выполнила свое обязательство по проведению оценки воздействия на защиту данных (DPIA).

# Иные санкции и меры принуждения





## 1001 Предписание о прекращении обработки данных



### ENFORCEMENT NOTICE

#### THE DATA PROTECTION ACT 2018 PART 6, SECTION 149

DATED 6 JULY 2018

To: AggregateIQ Data Services Ltd ("AIQ")

Of: 1200 Waterfront Centre  
200 Burrard Street  
P.O. Box 48600  
Vancouver BC V7X 1T2  
Canada

1. AIQ is a controller as defined in Article 4(7) of the General Data Protection Regulation EU2016/679 ("GDPR") and section 6 of the Data Protection Act 2018 ("DPA").
2. The provisions of the DPA and GDPR apply to the processing of personal data by AIQ ("the controller") by virtue of section 207(3) of the DPA and Article 3(2)(b) of the GDPR.
3. The Information Commissioner ("the Commissioner") has observed with concern the application of techniques hitherto reserved for commercial behavioural advertising being applied to political campaigning, during recent elections and the EU referendum campaign in 2016.
4. After initial preparatory evidence gathering, in May 2017 the Commissioner announced a formal investigation into the use of data analytics in political campaigning. The Commissioner is concerned that this has occurred without due legal or ethical consideration of the impacts to our democratic system.
5. The Commissioner has been in contact with AIQ regarding the processing of personal data by AIQ on behalf of UK political

## Enforcement Notice of the Information Commissioner, served under section 149 of DPA18, on AggregateIQ Data Services Ltd 6 July 2018

**Канадская** компания AggregateIQ Data Services, на основании статьи 3(2)(b) GDPR, получила предписание от британского регулятора прекратить обработку любых персональных данных граждан Великобритании или ЕС, полученных от политических организаций Великобритании или иных лиц, для целей аналитики данных, политической агитации или любых других рекламных целей.

Во Франции нарушение сроков хранения данных является уголовно наказуемым



### Уголовный кодекс Французской Республики ст.226-20

Хранение персональных данных сверх срока, установленного законом или нормативным актом, по заявлению о разрешении или заключении или по предварительному заявлению, направленному в Национальную комиссию по информационным технологиям и свободам (CNIL), наказывается пятью годами тюремного заключения и 300,000 евро, если такое хранение не осуществляется для исторических, статистических или научных целей на условиях, предусмотренных законом. Те же санкции применяются к факту, за исключением случаев, предусмотренных законом, обработки в иных целях, чем исторические, статистические или научные персональные данные, хранящиеся сверх срока, указанного в первом абзаце.

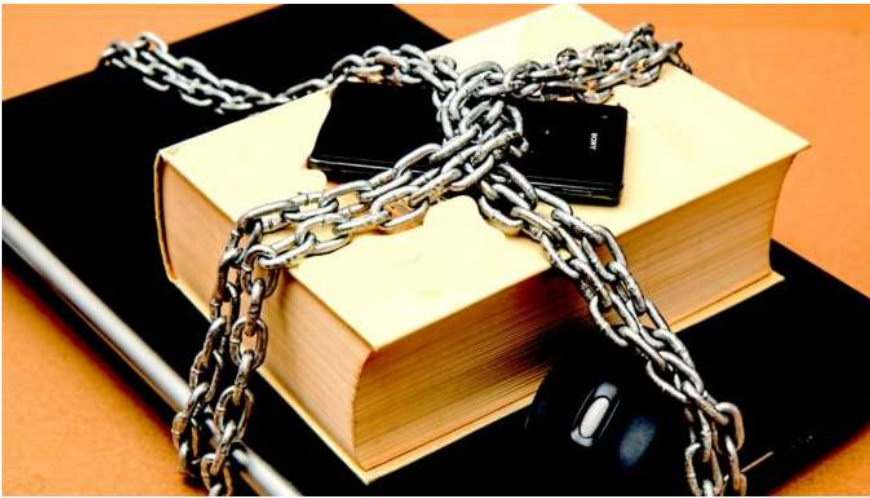
## Франция запрещает публикацию судебной аналитики, полученную в том числе с использованием технологий ИИ

### ARTIFICIAL LAWYER

CHANGING THE BUSINESS OF LAW

## France Bans Judge Analytics, 5 Years In Prison For Rule Breakers

© 4th June 2019 artificiallawyer Litigation Prediction 36



In a startling intervention that seeks to limit the emerging litigation analytics and prediction sector, the French Government has banned the publication of statistical information about judges' decisions – with a five year prison sentence set as the maximum punishment for anyone who breaks the new law.

Owners of legal tech companies focused on litigation analytics are the most likely to suffer from this new measure.

The new law, encoded in **Article 33** of the Justice Reform Act, is aimed at preventing anyone – but especially legal tech companies focused on litigation prediction and analytics – from publicly revealing the pattern of judges' behaviour in relation to court decisions.

Франция запретила публикацию судебной аналитики, а нарушение этого закона влечет за собой до пяти лет тюрьмы. Новая статья 33 Закона о реформе правосудия гласит: «Никакие персонально идентифицируемые данные, касающиеся судей или секретарей судебных заседаний, не подлежат повторному использованию с целью или результатом оценки, анализа или прогнозирования их фактической или предполагаемой профессиональной практики». Нарушение этого закона наказывается мерами, изложенными в статьях 226-18, 226-24 и 226-31 Уголовного кодекса.

В отличие от США и Великобритании, где судьи приняли как свершившийся факт активную работу юридических компаний, занимающихся использованием искусственного интеллекта для анализа судебных решений и построения на его основе достоверных предиктивных моделей, французские судьи решили бороться с ЭТИМ явлением.

## Предписание об изменении процесса обработки персональных данных



The screenshot shows the EDPB website with a news article titled "The Data Protection Ombudsman ordered Svea Ekonomi to correct its practices in the processing of personal data". The article is dated Wednesday, 24 April 2019. The text describes two cases concerning Svea Ekonomi, a financial credit company, processed at the Office of the Data Protection Ombudsman. The Ombudsman ordered the company to correct its practices in the processing of personal data related to the assessment of creditworthiness, the right of inspect one's own personal data and notification practices. The article details the Ombudsman's decision, stating that the use of a categorical upper age limit in assessing creditworthiness is not acceptable under the definition of credit information set out in the Credit Information Act. The mere age of the credit applicant does not describe their solvency, willingness to pay or ability to deal with their commitments. Based on the account submitted by the company, the credit applicant's financial position has not been taken into consideration at all in the automatic processing of the credit application. The Ombudsman also pointed out that the company's on-line credit decision service should be considered automatic decision-making of the kind referred to in Article 22 of the General Data Protection Regulation, in which the decision is essential in order to conclude or implement an agreement between the company and the credit applicant. In its decision, the Ombudsman ordered that Svea Ekonomi to change the processing of personal data related to assessing creditworthiness. The company must also provide the private person having complained about the matter with information on the logic employed in automatic decision-making, its role in making the credit decision as well as its consequences for the credit applicant. The procedure employed by Svea Ekonomi for assessing creditworthiness was also processed at the National Non-Discrimination and Equality Tribunal, which in its decision 216/2017, dated 21 March 2018, prohibited the company from repeating a procedure that is against the Equality Act and the Non-Discrimination Act. The Office of the Data Protection Ombudsman has also investigated Svea Ekonomi's notification practices related to the automatic decision-making system used to assess creditworthiness. The Ombudsman stated that the current notification practices do not sufficiently specify the logic of data processing so that the credit applicant could understand the grounds for the decision and ordered that such notification practices be changed. Based on the Ombudsman's decision, Svea Ekonomi must notify by 30 April 2019 how it has changed its processing of personal data. According to the Office of the Data Protection Ombudsman, Svea Ekonomi has not applied for change in the decision, so the decision is legally enforceable. Further information: Data Protection Ombudsman Reijo Aarnio, tel. +358 40 520 7068, reijo.aarnio[at]om.fi

## Tietosuoja-valtuutetun toimisto

Управление омбудсмена по защите данных в Финляндии Рейо Аарнио (Reijo Aarnio) выдало предписание компании «Svea Ekonomi», которая работает в сфере финансового кредитования, внести изменения, а также сделать более прозрачным и информативным для клиентов процесс оценки их кредитоспособности в соответствии с требованиями ст.22 GDPR.

## Временная блокировка обработки данных в приложении Норвежского института общественного здравоохранения



Норвежский надзорный орган выявил факт противоправной обработки персональных данных в приложения Smittestopp для отслеживания контактов с инфицированными COVID-19. Приложение собирает большие объемы данных о пользователях, в том числе локацию и информацию о контактах между пользователями. Регулятор предписал временно заблокировать обработку данных в приложении и пригласил контролера для обсуждения следующих вопросов:

- использование GPS (насколько это необходимо для целей приложения);
- внедрение решения по анонимизации данных;
- разработка решения по управлению запросами субъектов на доступ к их данным.

## Расширение для браузера «Shinigami Eyes» будет запрещено в Норвегии



Published: 12/21/2021

### «Shinigami Eyes» browser extension to be banned in Norway

The Norwegian Data Protection Authority has issued an advance notification of a ban on processing personal data by the browser extension «Shinigami Eyes», as the processing does not have a legal basis and insufficient information is provided to the data subjects.

- We believe that «Shinigami Eyes» has no legal basis for the processing of personal data, and we therefore intend to impose a ban on the browser extension in Norway, said Director-General Bjørn Erik Thon.

The Norwegian Data Protection Authority received several complaints against the browser extension «Shinigami Eyes», which is available for Chrome and Firefox. The browser extension seeks to highlight whether content and individuals are trans-friendly or transphobic.

#### Jeopardises freedom of expression

The Norwegian Data Protection Authority has assessed whether the use of the tool could be based on a balancing of interests as the legal basis. We have so far concluded that «Shinigami Eyes» does not have a legal basis for the processing of personal data.

Норвежский надзорный орган выпустил предварительное уведомление о запрете обработки персональных данных расширением для браузера «Shinigami Eyes», поскольку такая обработка не имеет правового основания и субъектам данных предоставляется недостаточно информации. Это расширение доступно для Chrome и Firefox и используется для определения степени транс-дружественности или трансфобности веб-контента и других пользователей.

Надзорный орган считает, что практика определения людей как транс-дружественных или трансфобных на основе субъективных оценок будет иметь негативные последствия для свободы выражения мнений в Интернете. Профилирование происходит тайно, без предоставления какой-либо информации профилируемому лицу, и что данное лицо не имеет возможности реализовать свое право на возражение.

## TikTok предписано блокировать пользователей, возраст которых невозможно подтвердить



**GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

### Tik Tok: dopo il caso della bimba di Palermo, il Garante privacy dispone il blocco del social

[English version](#)

Tik Tok: dopo il caso della bimba di Palermo, il Garante privacy dispone il blocco del social

Il Garante per la protezione dei dati personali [ha disposto nei confronti di Tik Tok il blocco immediato dell'uso dei dati degli utenti per i quali non sia stata accertata con sicurezza l'età anagrafica.](#)

L'Autorità ha deciso di intervenire in via d'emergenza a seguito della terribile vicenda della bambina di 10 anni di Palermo.

[Il Garante già a dicembre aveva contestato a Tik Tok una serie di violazioni:](#) scarsa attenzione alla tutela dei minori; facilità con la quale è aggirabile il divieto, previsto dalla stessa piattaforma, di iscriversi per i minori sotto i 13 anni; poca trasparenza e chiarezza nelle informazioni rese agli utenti; uso di impostazioni predefinite non rispettose della privacy.

In attesa di ricevere il riscontro richiesto con l'atto di contestazione, l'Autorità ha deciso comunque l'ulteriore intervento odierno al fine di assicurare immediata tutela ai minori iscritti ai social network presenti in Italia.

L'Autorità ha dunque vietato a Tik Tok l'ulteriore trattamento dei dati degli utenti "per i quali non vi sia assoluta certezza dell'età e, conseguentemente, del rispetto delle disposizioni collegate al requisito anagrafico".

Il divieto durerà per il momento fino al 15 febbraio, data entro la quale il Garante si è riservato ulteriori valutazioni.

Il provvedimento di blocco verrà portato all'attenzione dell'Autorità irlandese, considerato che recentemente Tik Tok ha comunicato di avere fissato il proprio stabilimento principale in Irlanda.

Roma, 22 gennaio 2021

---



### Tik Tok: Italian SA imposes limitation on processing after the death of the girl from Palermo

The Italian SA (Garante per la protezione dei dati personali) imposed an immediate limitation on the processing performed by TikTok with regard to the data of users whose age could not be established with certainty.

The SA decided to take urgent measures following the dismay caused by the death of a 10-year girl from Palermo:

[In December, the Garante had already notified several infringements](#) to TikTok including poor attention to the protection of minors, the easy dodging of the registration ban the company applies to children under 13 years, non-transparent and unclear information provided to users, and default settings falling short of privacy requirements.

Pending receipt of the feedback that was requested via the above notification, the Garante decided to anyhow step in today in order to afford immediate protection to the minors in Italy that have joined the social platform.

Итальянский надзорный орган (Il Garante per la protezione dei dati personali) предписал TikTok заблокировать учетные записи итальянских пользователей приложения, возраст которых не может быть достоверно подтвержден. Акт был принят после смерти 10-летней девочки от удушья в Палермо. Надзорный орган потребовал, чтобы приложение запрещало регистрацию любого пользователя младше 13 лет. Запрет продлится до передачи расследования ирландскую Комиссию по защите данных (как ведущему DPA).

## Предупреждение работодателю за GPS-мониторинг работников, использующих транспортные средства работодателя



**Кто:** Österreichische Datenschutzbehörde (Австрия)

**Кого:** неназванная компания

**Когда:** 2022.03

**За что:** нарушение ст.6 GDPR

**Как:** предупреждение (решение не окончательное)


**Причина:** расследование было начато после подачи жалобы работником компании, который был нанят в качестве специалиста по обслуживанию клиентов и ему было предоставлено служебное транспортное средство с устройством GPS-мониторинга, которое работник также мог использовать для личных поездок. Устройство активируется при включении зажигания транспортного средства и деактивируется при выключении зажигания, а в транспортном средстве имеется переключатель, с помощью которого устройство можно деактивировать во время личных поездок.

Надзорный орган установил отсутствие необходимости или соразмерности обработки данных системой GPS, отметив, что хотя GPS-мониторинг служит выгоде работодателя, но это само по себе не является обоснованием правомерности обработки данных на основе законного интереса работодателя, поскольку цель также может быть достигнута менее опасными для приватности работника способами.



## Garante per la protezione dei dati personali

Итальянский надзорный орган в сфере защиты персональных данных (Garante per la protezione dei dati personali) пригрозил руководству компании Mediamarket s.p.a. лишением свободы на срок от 3 месяцев до 2 лет в случае неисполнения предписания об использовании гранулированных согласий субъектов для маркетинговых активностей (включая программу лояльности) и прекращения обработки ранее собранных для таких активностей персональных данных.



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

### Provvedimento del 20 giugno 2019 [9124420]

VEDI ANCHE [Newsletter del 22 luglio 2019](#)

[doc. web n. 9124420]

Provvedimento del 20 giugno 2019

Registro dei provvedimenti  
n. 133 del 20 giugno 2019

#### IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito: "Regolamento UE");

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 106, di seguito "Codice"), modificato dal d.lgs. n. 101/2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE;

VISTE le segnalazioni inviate da XX all'Autorità ai sensi dell'art. 141, comma 1, lett. b), del Codice, con le quali l'interessata ha lamentato l'invio di comunicazioni promozionali indesiderate mediante posta elettronica da parte di Mediamarket s.p.a. (titolare del marchio "Mediaworld" di seguito anche "la Società");

VISTA l'analoga segnalazione presentata da XX;

VISTE le note inviate dalla Società e le risultanze dell'accertamento evoltesi presso la predetta Società, con l'ausilio del Nucleo Speciale Privacy della Guardia di Finanza;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Giovanna Bianchi Clerici;

#### PREMESSO

##### 1. Le segnalazioni pervenute all'Autorità

Sono pervenute all'Autorità segnalazioni da parte di XX (delle quali, la prima datata 15 giugno 2017 e l'ultima il settembre 2017), con le quali la medesima ha lamentato l'invio di comunicazioni promozionali mediante posta elettronica, da parte di Mediamarket s.p.a. (titolare del marchio "Mediaworld"), in assenza del necessario consenso e nonostante la reiterata opposizione dell'interessata ai sensi degli art. 7 ss. del Codice (effettuata, peraltro, in più modalità: contattando il servizio clienti, utilizzando la procedura di cancellazione dalla mailing list indicata nelle comunicazioni in questione; oppure, accedendo al sito web della Società).

In particolare è emerso che:

## Итальянский GDPR отклонил жалобу субъекта на отказ в реализации «права быть забытым»



Итальянский надзорный орган в сфере защиты персональных данных (Garante per la protezione dei dati personali) 16.12.2021 опубликовал свое решение по делу № 445, в котором он отклонил жалобу физического лица, попытавшегося реализовать свое право на удаление данных в соответствии со ст.17 GDPR. Причиной жалобы был отказ Google LLC удалить из результатов поиска статью с информацией о предыдущей общественной роли заявителя, а также критику назначения заявителя министром. Заявитель утверждал, что информация в статье больше не нужна в отношении целей, для которых она была первоначально обработана, поскольку заявитель более не является публичным лицом.

При рассмотрении жалобы надзорный орган руководствовался WP29 Guidelines on the Implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez' C-131/12 и EDPB Guidelines 5/2019 on the criteria of the Right to be Forgotten, согласно которым общественность должна иметь возможность искать информацию о субъектах, играющих роль в общественной жизни. И хотя статье уже три года, прошедшее короткое время не снижает интереса общественности к содержанию статьи.

## **В Норвегии больница не несет ответственности за медицинские данные после их разглашения иностранным лабораториям**

Норвежский совет по конфиденциальности («Personvernemnda») опубликовал 03.05.2022 года свое решение по делу № PVN-2021-21, в котором он постановил, что Oslo universitetssykehus HF («Университетская больница Осло») не несет ответственности за данные о состоянии здоровья пациентов после того, как они были медицинскому персоналу в иностранных лабораториях.

Дело касается жалобы Университетской больницы Осло на решение норвежского органа по защите данных ("Datatilsynet") от 26.04.2021, в котором Datatilsynet предписал больнице урегулировать раскрытие ею медицинской информации иностранным лабораториям в отдельных соглашениях об обработке данных (DPA) в соответствии со ст.28 GDPR или в соглашениях о совместном контроле (JCA) в соответствии со ст.26 GDPR. Основным спорным моментом заключается в том, остается ли больница контролером данных, предоставляемых иностранным лабораториям

Personvernemnda постановил, что правила, применяемые к обмену медицинской информацией с иностранными лабораториями на территории ЕС или ЕЭЗ, будут такими же, как и при отправке норвежским врачом медицинской информации в норвежские лаборатории, или при обмене данными между больницами в Норвегии, или при передаче данных зарубежным провайдерам медицинских услуг. Правила сотрудничества с медицинскими партнерами за рубежом, включая иностранные лаборатории, не могут быть более строгими, чем национальные правила, которые применяются к таким партнерам в соответствии со ст.1(3) GDPR.

Personvernemnda заключил, что доступ контролера, а во многих случаях и обязанность раскрывать медицинскую информацию медицинскому персоналу в иностранных лабораториях, исчерпывающе регулируется законодательством о здравоохранении, и что не может быть выдвинуто дополнительное требование о заключении соглашения в соответствии со ст. 26 и 28 GDPR.

Предписание Datatilsynet в адрес Университетской больницы Осло о заключении DPA или JCA было отменено.



The image shows a screenshot of a news article from the website 'Die Presse'. The article is titled '„Datenschutz systematisch verletzt“' (Data protection systematically violated). The author is identified as 'Salzburger Anwalt erklärt sein Vorgehen gegen reihenweise Online-Anbieter.' (Salzburg lawyer explains his approach against a series of online providers). The article discusses the actions of Peter Harlander, a lawyer from Salzburg, who is suing several online providers in Germany and Austria for systematic data protection violations. He demands 14,000 Euro for each company, 13,000 Euro for data protection violations, and 1,000 Euro for his own costs. The article also mentions that Harlander believes that many companies use tracking, profiling, and retargeting for profit optimization, and that many data protection bars are merely decorative.

**Die Presse** Nachrichten

Schnellauswahl Innenpolitik Ausland Economist Kultur Chronik Sport

# „Datenschutz systematisch verletzt“

Salzburger Anwalt erklärt sein Vorgehen gegen reihenweise Online-Anbieter.

**Wien/Salzburg.** „Es geht um gezieltes datenschutzwidriges Tracking, Profiling und Retargeting zum Zweck der Gewinnoptimierung im maximal denkbaren Umfang“: So erklärt Peter Harlander, warum er gegen mehrere Online-Anbieter in Deutschland und Österreich mit Schadenersatz- und Unterlassungsansprüchen vorgeht. Harlander ist jener Salzburger Rechtsanwalt, der (wie berichtet) für eine Mandantin von einem Unternehmen allein 14.000 Euro fordert (13.000 für Datenschutzverletzungen, 1000 für die eigenen Kosten).

Egal, ob man beim Surfen im Web den üblichen Datenschutzhinweis akzeptiere oder nicht - seine datenschutzaffinen Mandanten tun es nicht, sagt Harlander -, man werde beim Weitersurfen oft jedenfalls „von Werbung verfolgt“. Die meisten Datenschutz-Bars hätten „nur dekorative Wirkung“. Angesichts der Fülle an Informationen, die über die Nutzer gesammelt würden, findet der Anwalt 1000 Euro Schadenersatz je „Dienst“, an den sie weitergegeben würden (wie Facebook Pixel, Google DoubleClick), sogar moderat.

Питер Харландер, адвокат из Зальцбурга, от имени своих клиентов подал иски о возмещении убытков и судебном запрете на дальнейшую обработку персональных данных в соответствии со ст.82 GDPR против нескольких онлайн-провайдеров в Германии и Австрии. Харландер требует от каждой компании €10,000-13,000 (по €1,000 за каждый незаконно использованный cookie-файл) и еще €1,000 за собственные адвокатские услуги.

По словам адвоката, в исковых заявлениях идет речь о целевом отслеживании, профилировании и ретаргетинге пользователей сайтов с целью получения максимально возможной прибыли для компаний-владельцев сайтов. При этом разного рода баннеры и информационные сообщения об использовании cookies носят декоративный характер и фактически не препятствуют передаче данных пользователей сайтов третьим лицам (Facebook, Google и т.д.).

## Расследование EDPS в отношении Европарламента за использование сервисов NationBuilder



The screenshot shows the website of the European Data Protection Supervisor (EDPS). The header includes the EDPS logo and the text "EUROPEAN DATA PROTECTION SUPERVISOR" and "The EU's independent data protection authority". The navigation menu has "Home", "About", "Data Protection", and "Press & Publications". The breadcrumb trail reads "Home > ... > 2019 > EDPS investigates European Parliament's 2019 election activities and takes enforcement actions". The main heading is "EDPS investigates European Parliament's 2019 election activities and takes enforcement actions". A date stamp indicates "28 Nov 2019". A "Press Release" button is visible. The text of the press release states: "The European Data Protection Supervisor (EDPS) is carrying out an investigation into the European Parliament's use of a US-based political campaigning company to process personal data as part of its activities relating to the 2019 EU parliamentary election, the Assistant EDPS announced today." A quote from Wojciech Wiewiórowski, Assistant EDPS, is provided: "The EU parliamentary elections came in the wake of a series of electoral controversies, both within the EU Member States and abroad, which centred on the threat posed by online manipulation. Strong data protection rules are essential for democracy, especially in the digital age. They help to foster trust in our institutions and the democratic process, through promoting the responsible use of personal data and respect for individual rights. With this in mind, starting in February 2019, the EDPS acted proactively and decisively in the interest of all individuals in the EU to ensure that the European Parliament upholds the highest of standards when collecting and using personal data. It has been encouraging to see a good level of cooperation developing between the EDPS and the European Parliament over the course of this investigation." The text concludes: "Election campaigns are currently the subject of considerable scrutiny. The EDPS is actively engaged in seeking solutions to the challenges of online manipulation in elections while the European Parliament itself adopted a resolution to protect the European elections from data misuse in March 2019. Data protection plays a fundamental role in ensuring electoral integrity and must therefore be treated as a priority in the planning of any election campaign."

**Кто:** European Data Protection Supervisor (EDPS)

**Кого:** Европейский парламент

**Когда:** 2019.11

**За что:** нарушение ст.29 Regulation (EU) 2018/1725

**Как:** два выговора (reprimands)

**Причина:** Европейский парламент использовал NationBuilder в качестве обработчика данных для публичной кампании по привлечению общественности к участию в голосовании на весенних выборах 2019 года, которая проводилась посредством веб-сайта [thistimeimvoting.eu](http://thistimeimvoting.eu) и привела к обработке данных более чем 329,000 человек. Первый выговор был вызван неосведомленностью Европарламента о содержании и о специфике процесса обработки данных со стороны NationBuilder, а второй выговор был вынесен по причине не соблюдения предписания EDPS о публикации Политики конфиденциальности на веб-сайте [thistimeimvoting.eu](http://thistimeimvoting.eu).

## EDPS предписал Европолу удалить персональные данные, непосредственно не связанные с преступлениями



The image shows a screenshot of a press release from the European Data Protection Supervisor (EDPS). At the top left, there is the EDPS logo, which includes the European Union flag and the text 'EDPS EUROPEAN DATA PROTECTION SUPERVISOR'. The main headline reads: 'EDPS orders Europol to erase data concerning individuals with no established link to a criminal activity'. Below the headline, there is a date stamp '10 Jan 2022' and a 'Press Release' button. The text of the press release states: 'On 3 January 2022, the EDPS notified Europol of an order to delete data concerning individuals with no established link to a criminal activity (Data Subject Categorisation). This Decision concludes the EDPS' inquiry launched in 2019.' It further explains that the EDPS admonished Europol in September 2020 for the continued storage of large volumes of data with no Data Subject Categorisation, which poses a risk to individuals' fundamental rights. The EDPS has decided to use its corrective powers and to impose a 6-month retention period (to filter and to extract the personal data). Datasets older than 6 months that have not undergone this Data Subject Categorisation must be erased. This means that Europol will no longer be permitted to retain data about people who have not been linked to a crime or a criminal activity for long periods with no set deadline. The EDPS has granted a 12-month period for Europol to comply with the Decision for the datasets already received before this decision was notified to Europol.

**Кто:** European Data Protection Supervisor (EDPS)

**Кого:** Европол

**Когда:** 2022.01

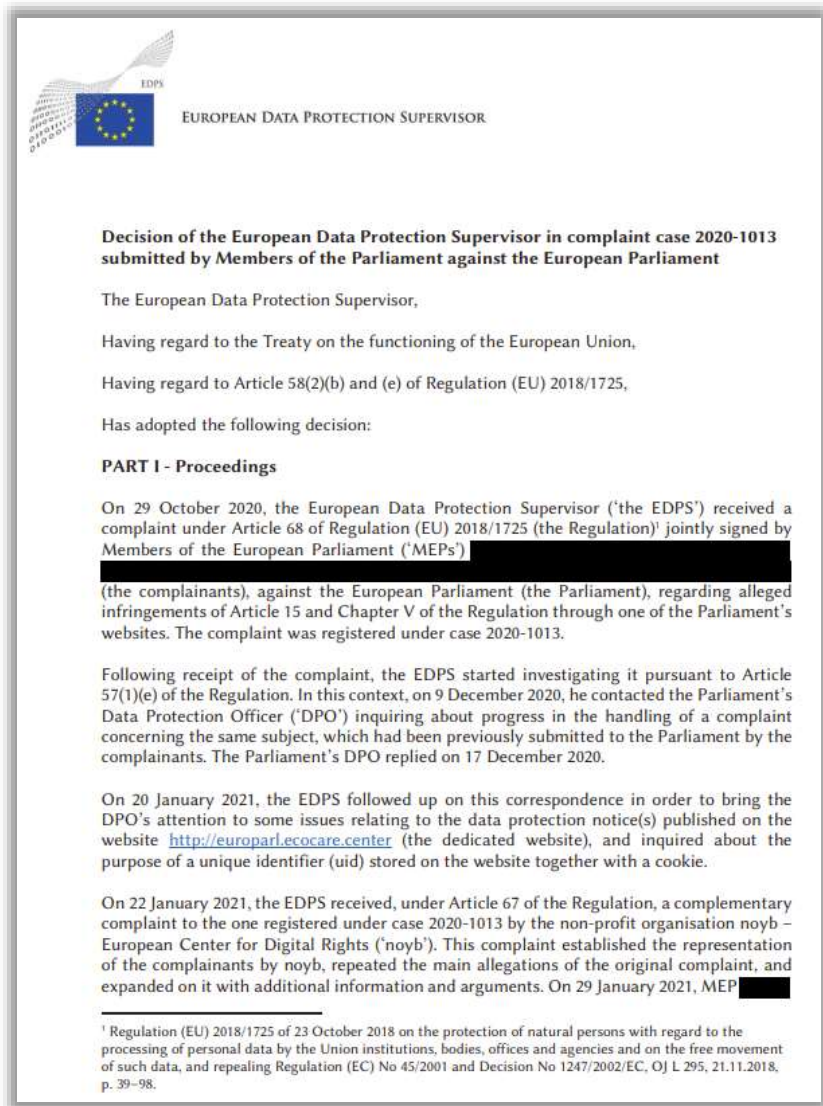
**За что:** нарушение ст. 28(1)(e) Regulation (EU) 2016/794 (Europol Regulation)

**Как:** предписание удалить избыточные данные, не связанные с криминальными расследованиями, в течение одного года

**Причина:** общий объём сведений, хранящихся в базах Европола, приблизительно оценивается в 4 петабайта. В базах содержатся сведения о как минимум четверти миллиона подозреваемых в террористической активности и серьёзных преступлениях, а также информация о других людях, связанных с подозреваемыми. Данные получены из всевозможных правоохранительных ведомств стран ЕС.

Персональные данные зачастую хранились и обрабатывались без достаточных оснований, в результате чего резиденты ЕС могли быть ошибочно связаны с криминальной активностью. База данных Европола как минимум частично состоит из сведений о людях, не являющихся «подозреваемыми», «потенциальными будущими преступниками», «лицами находящимися в контакте или связанными с преступниками», «жертвами», «свидетелями» или «информаторами».

## Предписание EDPS в отношении Европарламента за использование сервисов из США на сайте для тестирования COVID-19



**Кто:** European Data Protection Supervisor (EDPS)

**Кого:** Европейский парламент

**Когда:** 2022.01

**За что:** нарушение ст. 4(1)(a), 4(2), 14, 17, 26(1), 29(1), 29(3), 37, 46, 48(2)(b) Regulation (EU) 2018/1725

**Как:** предписание исправить нарушение в течение одного месяца

**Причина:** в 2020 году Европарламент нанял компанию Stripe, чтобы провести массовое тестирование парламентариев и официальных лиц с использованием специального веб-сайта на наличие COVID-19. Однако EDPS обнаружил, что в ходе этого процесса не соблюдались строгие ограничения на передачу информации через Атлантику – на веб-сайте парламента были размещены трекеры, через которые обрабатывались персональные данные, эта информация впоследствии передавалась в США, где базируются Stripe и Google.

Парламент не предоставил никакой документации, доказательств или иной информации относительно договорных, технических или организационных мер, принятых для обеспечения по существу эквивалентного уровня защиты персональных данных, передаваемых в США в контексте использования файлов cookie на веб-сайте.

## Предупреждение и предписание физическому лицу за нарушение принципа минимизации данных

**Кто:** Agencia Española de Protección de Datos (Испания)

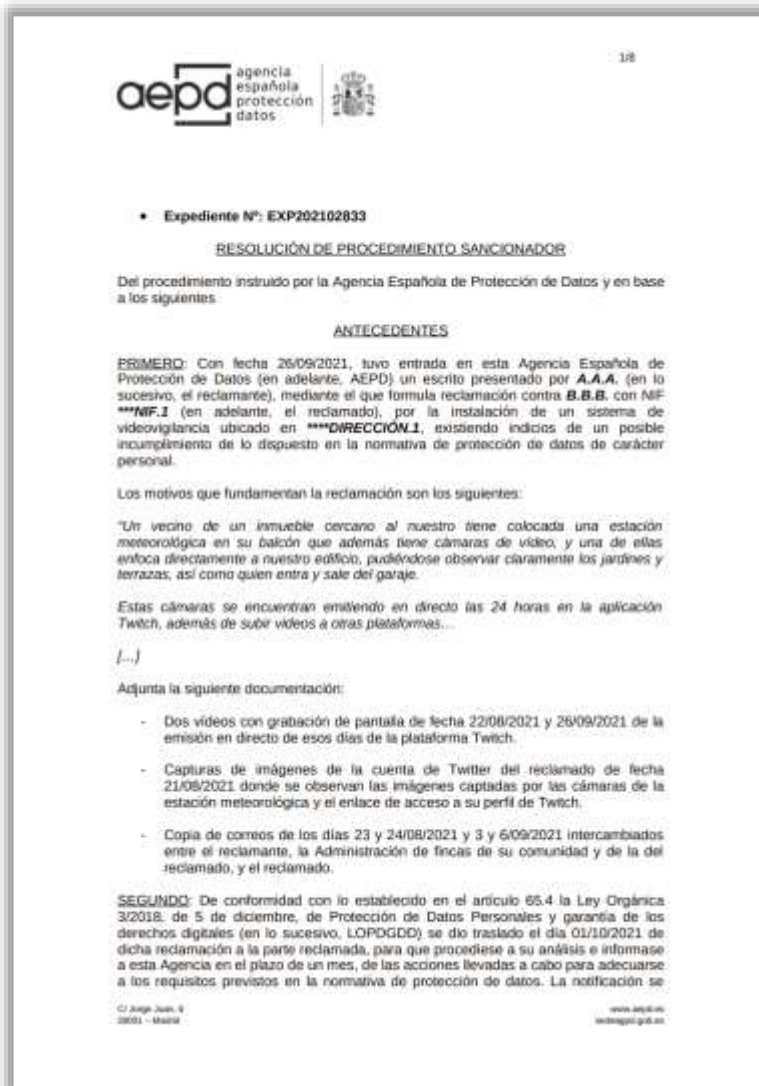
**Кого:** неназванное физическое лицо

**Когда:** 2022.04

**За что:** нарушение ст. 5(1)(c) GDPR

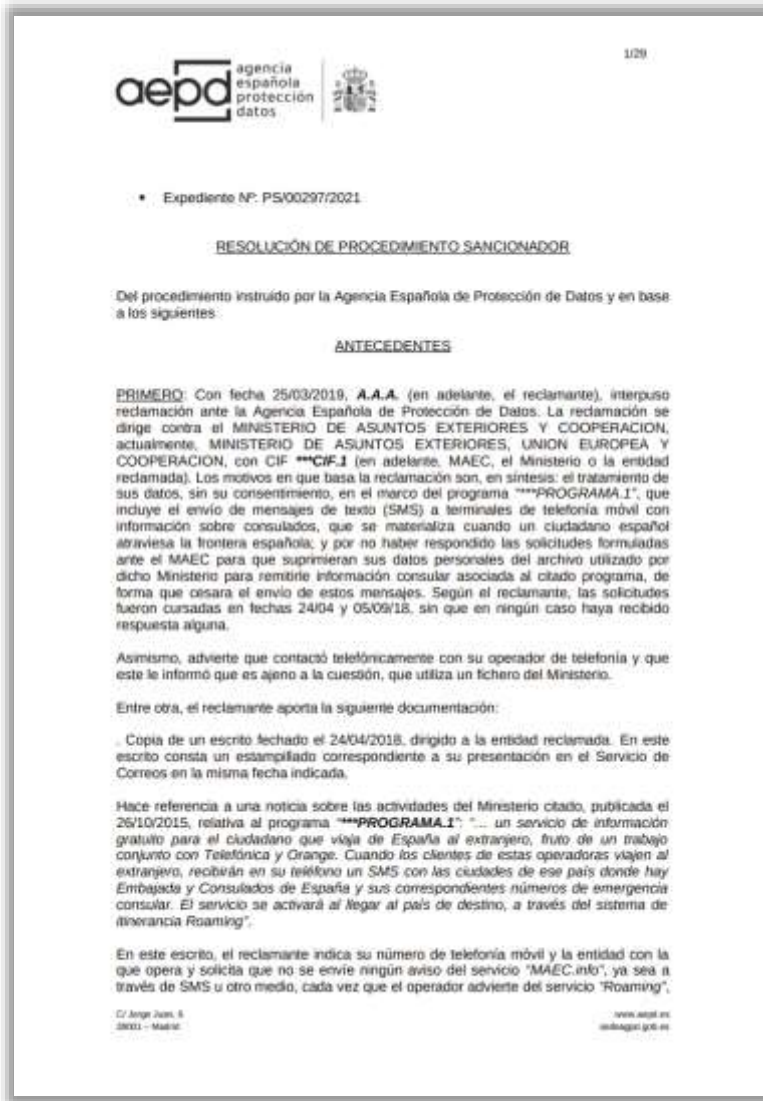
**Как:** предупреждение + предписание в течение 10 дней перенести метеостанцию или перенастроить систему видеонаблюдения

**Причина:** установка физическим лицом по месту своего жительства метеостанции с системой видеонаблюдения, состоящей как минимум из четырех камер, фиксирующей окружающую местность, включая прилегающие здания и перемещение людей/транспорта. Кроме того, видеотрансляция была общедоступной на платформах социальных сетей.





## Предупреждение и предписание Министерству иностранных дел за несоблюдение права на возражение и отсутствие DPA



**Кто:** Agencia Española de Protección de Datos (Испания)

**Кого:** Министерство иностранных дел Испании (МАЕС)

**Когда:** 2022.05

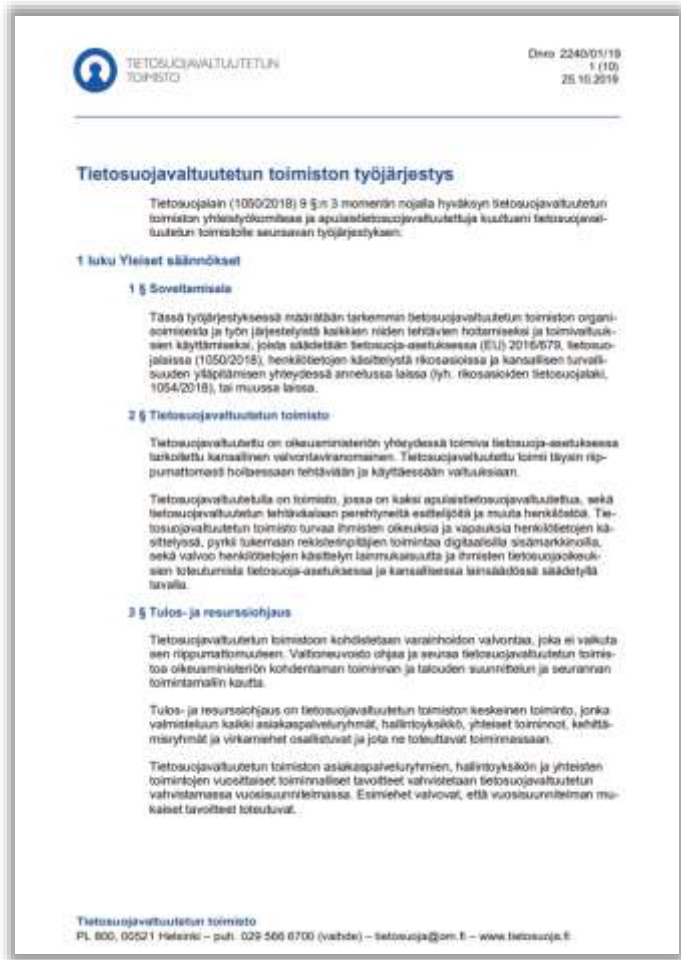
**За что:** нарушение ст. 21, 28(3) GDPR

**Как:** предупреждение + предписание в течение 3 месяцев устранить нарушения

**Причина:** данные граждан Испании обрабатывались без их согласия в рамках разработанной МАЕС бесплатной информационной услуги для лиц, путешествующих из Испании за границу, и которая заключалась в отправке SMS-сообщений на их мобильные телефоны с номерами экстренных служб посольств и консульств Испании, расположенных в городах посещения. Кроме того, субъекты данных направляли в МАЕС запросы с просьбой отказаться от получения SMS-сообщений, связанных с этой программой, а также удалить свои персональные данные, хранящиеся для этой цели, на которые МАЕС не ответил.

Кроме того, между МАЕС и операторами связи, отвечающими за отправку SMS-сообщений, не было заключено Data Processing Agreement.

# 1018 Отказ в доступе к данным истории ремонта и обслуживания автомобиля



**Кто:** Tietosuojavaltuutetun toimisto (Финляндия)

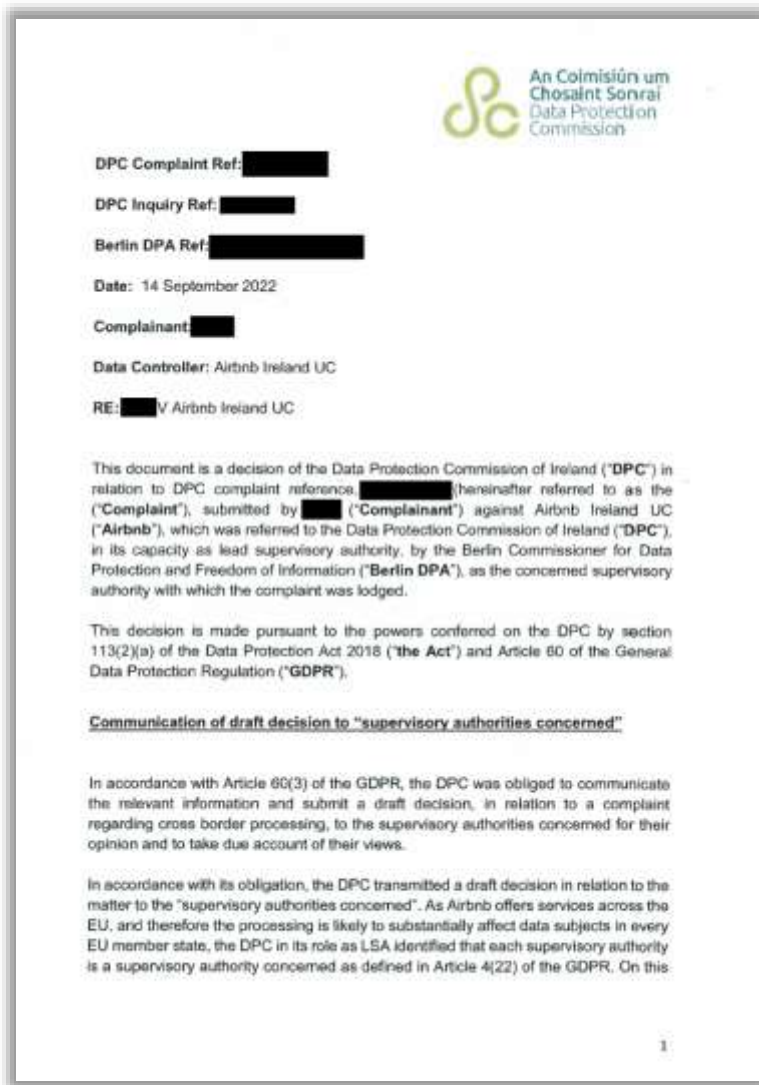
**Когда:** 2022.06

**Причина:** лицо, купившее подержанный автомобиль, сообщило DPA, что оно запросило у BMW Suomi информацию об истории технического обслуживания и ремонта на протяжении всего жизненного цикла автомобиля, однако BMW Suomi не предоставила никакой запрашиваемой информации.

DPA посчитал, что данные об истории технического обслуживания автомобиля в принципе являются персональными данными по смыслу GDPR, которые относятся к владельцу автомобиля в период владения им. Данные истории обслуживания могут прямо или косвенно описывать владельца транспортного средства или его деятельность, заявив, однако, что некоторые данные истории обслуживания могут быть и не персональными данными. При этом история обслуживания автомобиля не является персональными данными нового владельца автомобиля, и поэтому новый владелец не имеет права получить эти данные на основании права доступа.

Однако DPA не оценивал право BMW Suomi предоставить данную информацию на каком-либо другом основании, кроме права доступа (DSAR – ст.15 GDPR) и решил, что GDPR в принципе не препятствует раскрытию данных об истории обслуживания и ремонта автомобиля лицу, купившему подержанный автомобиль, отметив, что это может быть возможно, например, в контексте законного интереса в соответствии с GDPR.

## 1019 Выговор за нарушение принципа минимизации данных



**Кто:** Data Protection Commission (Ирландия)

**Кого:** Airbnb Ireland UC

**Когда:** 2022.09

**За что:** нарушение ст. 5(1)(с), 6(1), 12(3) GDPR

**Как:** выговор и предписание устранить нарушения GDPR за 3 месяца

**Причина:** Airbnb не выполнил запрос на удаление данных и последующий запрос на доступ к ним в установленные законом сроки. Когда заявитель подал запрос на удаление данных, Airbnb попросила его подтвердить свою личность, предоставив ксерокопию удостоверения личности, которое он ранее не предоставлял Airbnb, при этом у компании были альтернативные способы идентификации обратившегося лица.

DPC предписал Airbnb, в соответствии со Статьей 5(1)(с) GDPR, пересмотреть свою внутреннюю политику и процедуры обработки запросов на удаление данных, чтобы гарантировать, что от частных лиц больше не требуется предоставлять копию фотографического удостоверения личности при подаче запросов на удаление данных, если только Airbnb не сможет доказать наличие законных оснований для этого.

## Временная блокировка обработки данных на платформе Replika из-за рисков для несовершеннолетних лиц



**Provvvedimento del 2 febbraio 2023 [9852214]**

VEDI ANCHE: [Comunicato stampa del 3 febbraio 2023](#)



- [English version](#)  
[doc. web n. 9852214]

Provvvedimento del 2 febbraio 2023

Registro dei provvvedimenti  
n. 39 del 2 febbraio 2023

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito, "Regolamento");

VISTO altresì il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196);

RILEVATO che recenti notizie di stampa hanno dato evidenza – con dovizia di dettagli – di alcune prove condotte sull'applicazione Replika (una chatbot, con interfaccia scritta e vocale, basata sull'intelligenza artificiale che genera un "amico virtuale" che l'utente può decidere di configurare come amico, partner romantico o mentore), prove che hanno evidenziato concreti rischi per i minori d'età e, più in generale, per le persone in stato di fragilità emotiva;

RILEVATO che nella privacy policy (aggiornata al 5 luglio 2022) pubblicata nel suo sito web, il fornitore del servizio dichiara di non raccogliere consapevolmente dati personali di minori di età inferiore ai 13 anni ed incoraggia i genitori e i tutori legali a monitorare l'utilizzo di Internet da parte dei propri figli, a rispettare la privacy policy istruendo i minori a non fornire mai dati personali sul servizio senza la loro autorizzazione e a contattare la piattaforma nell'ipotesi in cui abbiano motivo di ritenere che un bambino di età inferiore ai 13 anni abbia fornito dati personali affinché questi possano essere eliminati dai database;

RILEVATO, in particolare, che nei due principali "App store" l'applicazione viene classificata come idonea a persone maggiori di 17 anni, mentre, nei termini di servizio (aggiornati al 14 settembre 2022) pubblicati nel sito web dello sviluppatore viene indicato un divieto di utilizzo per i minori di 13 anni e l'esigenza che i minori di 18 anni siano previamente autorizzati da un genitore o da un tutore;

CONSIDERATO che dalle prove condotte e riportate dai richiamati articoli di stampa emerge l'assenza di filtri per i minori di età e la proposizione ad essi di risposte assolutamente inidonee rispetto al grado di sviluppo e autoconsapevolezza degli stessi;

VERIFICATO che durante la fase di creazione di un account la piattaforma non prevede alcuna

**Kto:** Garante per la protezione dei dati personali (Italia)

**Kogo:** Luka, Inc. (владелец платформы Replika)

**Kогда:** 2023.02

**За что:** нарушение ст. 5, 6, 8, 9, 13, 25 GDPR

**Как:** временное ограничение обработки персональных данных итальянцев в мобильном приложении Replika + 20 дней на устранение выявленных нарушений

**Причина:** сообщения в прессе о том, что мобильное приложение Replika – чат-бот с текстовым и голосовым интерфейсом, который на основе искусственного интеллекта создает «виртуального друга» – порождает риски для несовершеннолетних лиц и, в целом, для людей, находящихся в состоянии эмоциональной неустойчивости.

Garante указал на отсутствие фильтров контента для несовершеннолетних, что приводит к предложению им абсолютно неподходящих ответов с учетом степени их развития и самосознания, а также на то, что при создании аккаунта платформа не предусматривает никакой процедуры верификации и проверки возраста пользователя. Политика конфиденциальности Replika не соответствует принципам GDPR в отношении прозрачности.

## Претензия в адрес американской корпорации Alphabet от германского Федерального ведомства по делам картелей

Германское Федеральное ведомство по делам картелей ('Bundeskartellamt') 11.01.2023 направило официальную претензию в адрес американской корпорации Alphabet, в которой раскритиковало ее политику по управлению персональными данными пользователей.

"Заявление о несогласии [с политикой компании] было направлено 23 декабря в адрес Alphabet Inc (США), а также ее дочерних подразделений в Ирландии и Германии - Google Ireland и Google Germany. Мы полагаем, что [американская корпорация] должна изменить условия сбора и обработки персональных данных пользователей и связанные с этим процедуры", - указано в документе.

В частности, эксперты регулятора в ходе оценки практик Alphabet пришли к выводу, что американская компания "не предоставляет пользователям достаточных полномочий по распоряжению своими данными". Существующие в продуктовой экосистеме корпорации варианты управления подобной информацией "недостаточно прозрачны", а компания "лишь в общих чертах" обозначает то, как и для чего именно она собирает и обрабатывает личные данные.

Наибольшую обеспокоенность ведомства вызвал тот факт, что американская корпорация проводит анализ данных, "одновременно поступающих в ходе использования всех ее продуктов", среди которых значатся как электронные устройства (смартфоны, работающие на базе системы Android), так и сервисы (поисковик Google, электронная почта Google Mail) и приложения (YouTube, Google Maps и прочие). Представители регулятора полагают, что такой комплексный подход позволяет Alphabet "составлять подробные профили на пользователей", которые она затем может применять "для таргетирования рекламы и иных целей". К подобной практике "недопустимо прибегать без достаточных на то оснований", исключение могут составить лишь ситуации, когда это "необходимо для обеспечения безопасности", считают эксперты ведомства.

В связи с этим представители регулятора призвали американскую компанию внести изменения в политику управления данными пользователей, предоставив им возможность самим ограничивать сбор и обработку данных рамками каждого конкретного приложения или сервиса. Они обратили внимание на то, что официальное заявление о несогласии стало "первым промежуточным шагом в административном производстве" ведомства против Alphabet. Теперь корпорация может ответить на изложенные претензии, после чего регулятор вынесет суждение о том, достаточно ли у нее оснований для проведения текущей политики управления личными данными клиентов.

Ожидается, что ведомство примет соответствующее решение до конца 2023 года. В полномочия регулятора входит наложение официальных обязательств на цифровые компании в области политики управления персональными данными пользователей, уточняется в его заявлении.

## Контролёр не обязан представлять субъектам сведения о мерах безопасности и о нарушениях безопасности данных



Решение бельгийского органа по защите данных (l'Autorité de protection des données) о пределах доступа к запросам субъектов данных в случае, когда субъект данных жаловался, что ответ был (i) несвоевременным и (ii) неполным.

- (i) Ответ был получен с опозданием из-за длительного отсутствия лица, обычно управляющего запросами субъектов данных, по причине болезни, в результате чего запрос на доступ был забыт. DPA заявил, что это не оправдывает несвоевременный ответ. Тем не менее, контролер принял меры для того, чтобы подобное не повторилось (создание специального почтового ящика для запросов, чтобы несколько человек имели доступ к таким запросам). Итог: контролеру объявлен выговор, а не назначен штраф.
- (ii) Контролер отказался ответить на некоторые вопросы, заданные субъектом данных, например, были ли какие-либо нарушения данных и какие меры безопасности были приняты. DPA подтвердил, что контролер имел право отказать в предоставлении информации о мерах безопасности, поскольку эта тема не охватывается статьями 13(1), 13(2) или 15(1) GDPR. DPA также подтвердил, что нет необходимости предоставлять информацию о нарушениях безопасности данных, так как нет никаких указаний на то, что в отношении субъекта данных были какие-либо нарушения данных с высоким риском.

## Чешское UOOU предписало удалить списки адресов электронной почты физических лиц из системы открытых данных

**Úřad pro ochranu osobních údajů**

Základní odkazy | O NÁS • NÁZORY A ROZHODNUTÍ ÚŘADU • TISKOVÉ ZPRÁVY

### Seznamy majitelů datových schránek zmizí ze systému otevřených dat

Ze systému otevřených dat budou odstraněny seznamy nepodnikajících fyzických osob, které byly dosud zveřejněny na webu Datových schránek a v Národním katalogu otevřených dat. Dohodli se na tom představitelé Úřadu pro ochranu osobních údajů (ÚOOÚ) a Digitální a informační agentury (DIA).

Úřad pro ochranu osobních údajů konstatoval, že seznam datových schránek fyzických osob je zveřejněn nejen v podobě formuláře pro vyhledávání konkrétní datové schránky na stránkách [www.mojedatovyschranka.cz](http://www.mojedatovyschranka.cz), ale současně také v rámci systému tzv. „otevřených dat“.

Seznam držitelů datových schránek tak byl zveřejněn „způsobem umožňujícím dálkový přístup v otevřeném a strojově čitelném formátu“. Zjednodušeně řečeno byly tyto otevřené datové sady přizpůsobeny pro neomezené stahování a kopírování stejně jako pro další využití. Tato funkcionality byla přitom dostupná komukoli, a to bez jakékoli kontroly nebo regulace takového užití.

Úřad pro ochranu osobních údajů proto upozornil zřizovatele a správce systému datových schránek Ministerstvo vnitra na to, že s ohledem na zásady zpracování osobních údajů podle GDPR – zejména pak ve vztahu k zásadě minimalizace a důvěrnosti zpracování osobních údajů – je uveřejnění takového seznamu údajů nepřijatelné.

Agendu datových schránek od 1. dubna 2023 převzala Digitální a informační agentura (dále jen „DIA“), která na výzvu Úřadu pro ochranu osobních údajů reagovala obratem a jako nový garant provozu datových schránek (a tedy i správce osobních údajů uvedených v daném seznamu) okamžitě zahájila kroky k odstranění této otevřené datové sady ze systému.

Otevřená data na jedné straně představují vysoce efektivní způsob zveřejňování informací veřejného sektoru, Úřad pro ochranu osobních údajů však dlouhodobě poukazuje na nevhodnost tohoto způsobu zveřejňování, pokud jde o osobní údaje. Úvodem přitom není samotná otázka zveřejnění (otevřená data zahrnují údaje z veřejných rejstříků), ale následná libovolná a neomezená dispozice s celými datovými soubory, která podle názoru ÚOOÚ není slučitelná s ochranou osobních údajů.

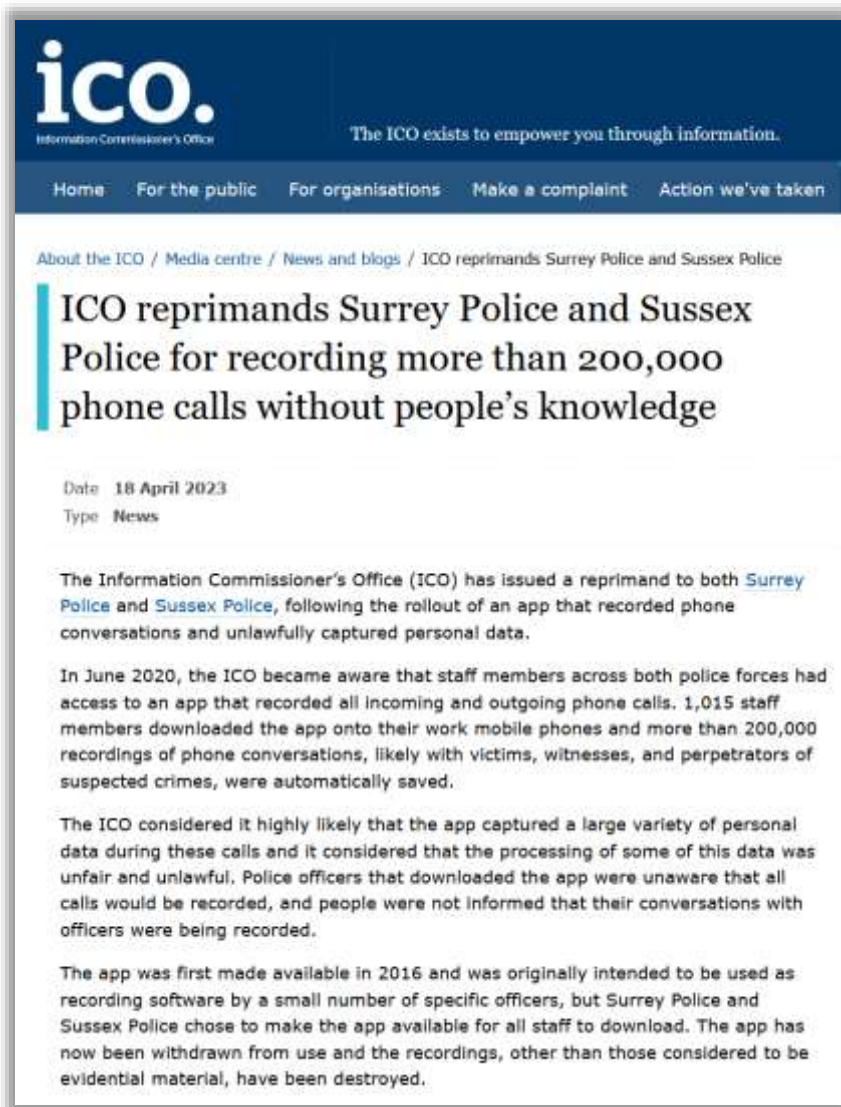
Na společném jednání zástupců ÚOOÚ a DIA byla rovněž dohodnuta spolupráce při přípravě odpovídající úpravy stávající legislativy směřující ke zpřístupnění údajů o datových schránkách fyzických osob pouze uživatelům datových schránek. Téma zveřejnění a rozsah údajů související s datovými schránkami podnikajících fyzických osob přitom bude předmětem dalších jednání.

◇ Чешское Управление по защите персональных данных ("UOOU") 14.04.2023 заявило, что списки адресов электронной почты физических лиц, не являющихся предпринимателями, будут удалены из системы открытых данных в Чехии, так как это позволяло неограниченное скачивание, копирование и использование в нарушение требований GDPR.

◇ UOOU указало Министерству внутренних дел Чехии, как первоначальному владельцу и администратору открытой системы данных, что публикация таких данных неприемлема в отношении принципа минимизации и конфиденциальности обработки персональных данных. С 01.04.2023 Агентство цифровых и информационных технологий ("DIA") начало удалять из системы открытого набора данных, содержащего адреса электронной почты физических лиц.

◇ Управление по защите персональных данных раскритиковало непригодность систем открытых данных для обработки персональных данных, так как последующее неограниченное распоряжение целыми наборами данных не совместимо с защитой персональных данных, несмотря на их эффективность в публикации информации государственного сектора.

## Британское ICO вынесло выговор полиции Сассекса и полиции Суррея за незаконное хранение записей телефонных разговоров



The screenshot shows the top of the ICO website with the logo and tagline. Below is a navigation menu and a breadcrumb trail. The main headline is 'ICO reprimands Surrey Police and Sussex Police for recording more than 200,000 phone calls without people's knowledge'. The article text follows, detailing the reprimand issued to both police forces for using an app that recorded phone calls without consent.

**ico.**  
Information Commissioner's Office  
The ICO exists to empower you through information.

Home For the public For organisations Make a complaint Action we've taken

About the ICO / Media centre / News and blogs / ICO reprimands Surrey Police and Sussex Police

### ICO reprimands Surrey Police and Sussex Police for recording more than 200,000 phone calls without people's knowledge

Date 18 April 2023  
Type News

The Information Commissioner's Office (ICO) has issued a reprimand to both [Surrey Police](#) and [Sussex Police](#), following the rollout of an app that recorded phone conversations and unlawfully captured personal data.

In June 2020, the ICO became aware that staff members across both police forces had access to an app that recorded all incoming and outgoing phone calls. 1,015 staff members downloaded the app onto their work mobile phones and more than 200,000 recordings of phone conversations, likely with victims, witnesses, and perpetrators of suspected crimes, were automatically saved.

The ICO considered it highly likely that the app captured a large variety of personal data during these calls and it considered that the processing of some of this data was unfair and unlawful. Police officers that downloaded the app were unaware that all calls would be recorded, and people were not informed that their conversations with officers were being recorded.

The app was first made available in 2016 and was originally intended to be used as recording software by a small number of specific officers, but Surrey Police and Sussex Police chose to make the app available for all staff to download. The app has now been withdrawn from use and the recordings, other than those considered to be evidential material, have been destroyed.

Британское Управление комиссара по информации ("ICO") 03.04.2023 вынесло выговор полиции Сассекса и полиции Суррея за нарушение разделов 35(1) и 45(1) Закона о защите данных 2018 года (UK Data Protection Act 2018).

◇ Сотрудники обеих полицейских служб использовали мобильное приложение, которое записывало все входящие и исходящие телефонные звонки, что привело к автоматическому сохранению более 200,000 записей телефонных разговоров, вероятно, с жертвами, свидетелями и лицами, подозреваемыми в совершении преступлений. Кроме того, сотрудники полиции, загрузившие приложение, не знали о том, что все звонки будут записываться, в то время как отдельные лица не были проинформированы о том, что их разговоры с сотрудниками записываются.

◇ ICO рекомендовало обоим полицейским органам принять меры по обеспечению соблюдения ими законодательства о защите данных и потребовало в течение трех месяцев после вынесения выговоров предоставить подробную информацию о мерах, принятых для выполнения этих рекомендаций.



## Румынский ANSPDCP вынес выговор за использование WhatsApp в качестве официального канала связи с потребителями

Орган по защите персональных данных Румынии (ANSPDCP) принял корректирующие меры в отношении Национального управления по защите прав потребителей Румынии за использование WhatsApp в качестве официального канала связи с потребителями без принятия технических и организационных мер в соответствии со ст. 32 GDPR.

Национальное управление по защите прав потребителей (ANPC) - контролер - приняло решение о предоставлении специального номера мобильного телефона для отправки жалоб потребителей через сообщения WhatsApp. В контексте нескольких обращений и уведомлений по этому каналу контроллер собрал большое количество персональных данных. После рассмотрения нескольких жалоб на эту практику, а также новостей, опубликованных в различных СМИ, ANSPDCP инициировал расследование по факту использования WhatsApp ANPC.

В результате расследования ANSPDCP установил, что ANPC собирала персональные данные через WhatsApp, который не находился под ее контролем, не принимая во внимание потенциальные риски для субъектов данных. ANSPDCP подчеркнул, что у ANPC уже были другие доступные каналы для подачи заявлений и жалоб, такие как зарегистрированный электронный ящик или форма на сайте учреждения.

Таким образом, ANSPDCP установил, что ANPC нарушила ст. 32(2) GDPR, и вынес выговор, а также принял меры по исправлению ситуации, чтобы обработка персональных данных осуществлялась только с использованием средств, находящихся под контролем ANPC. Эти меры также включали в себя внедрение соответствующих технических и организационных мер, гарантирующих и способных продемонстрировать, что обработка осуществляется в соответствии с положениями GDPR.

## Ирландский DPC вынес компании Airbnb Ireland выговор и предписание об устранении недостатков за незаконную обработку персональных данных

DPC начал свое расследование 04.03.2022 в связи с жалобой на то, что Airbnb Ireland незаконно запросила копию удостоверения личности заявителя для проверки его личности, которая ранее не запрашивалась Airbnb. Заявитель также утверждал, что это противоречит принципам минимизации данных и что Airbnb также не соблюдает принципы прозрачности и предоставления информации. Первоначальные попытки заявителя подтвердить свою личность были отклонены Airbnb, поскольку предоставленный им идентификатор не соответствовал их критериям, однако в конечном итоге заявитель подтвердил свою личность.

Поскольку рассматриваемая ситуация представляет собой трансграничную обработку, в соответствии со ст.60(3) GDPR, DPC направил свой проект решения в соответствующие надзорные органы для получения их мнения. В установленный законом срок он не получил от соответствующих надзорных органов каких-либо релевантных и обоснованных возражений по проекту решения.

В результате проведенного расследования DPC установил, что сохранение компанией Airbnb копии документов, удостоверяющих личность заявителя, после успешного завершения процесса проверки личности нарушает принципы минимизации данных, предусмотренные ст.5(1)(c) GDPR, и принцип ограничения хранения данных, предусмотренный ст.5(1)(e) GDPR. Кроме того, дальнейшая обработка и хранение частично отредактированных и устаревших документов, удостоверяющих личность, которые были признаны неадекватными или недостаточными для проверки личности заявителя, также нарушает принципы минимизации данных и ограничения хранения данных.

DPC вынес следующие предписания в отношении Airbnb Ireland:

1. удалить из всех своих систем и записей отредактированные и устаревшие копии документов, удостоверяющих личность заявителя, которые он пытался загрузить;
2. удалить из всех своих систем и записей документы, удостоверяющие личность, которые были загружены заявителем (сохранив только запись о том, что такие документы были представлены, а также дату их представления);
3. при условии соблюдения законодательства ЕС и государств-членов ЕС пересмотреть свои внутренние политики и процедуры, касающиеся проверки личности пользователя, с тем чтобы:
  - 3.1. после того, как личность субъектов данных была подтверждена к удовлетворению Airbnb Ireland, Airbnb Ireland прекращает практику сохранения неправильно отредактированных и/или устаревших документов, удостоверяющих личность, которые могут быть представлены субъектами данных в рамках процесса проверки личности;
  - 3.2. срок хранения действительных, мошеннических или незаконных документов, удостоверяющих личность (включая документы, удостоверяющие личность, отредактированные в соответствии с законами, требующими определенного редактирования), предоставленных субъектами данных в рамках процесса проверки личности, ограничен строгим минимумом (в соответствии с п.39 преамбулы к GDPR).

## Греческий НДПА решил, что генеалогическое исследование фамилии не подпадает под действие ст. 15 GDPR

5 августа 2022 года субъект данных подал жалобу на Direktorat начального образования. Субъект данных хотел провести генеалогическое расследование по своей фамилии. Он отправил электронное письмо в Управление начального образования (контролер) с просьбой предоставить ему доступ к базе данных регистрации учеников для поиска в ней записей о его фамилии. Кроме того, в своей жалобе субъект данных просил Управление обязать Direktorat начального образования предоставить ему немедленный доступ к учебникам закрытой/уничтоженной начальной школы для поиска в них записей о его фамилии. Контролер ответил, что может предоставить ему только числовые данные (количество учеников в год), но не фамилии, так как это было бы незаконным раскрытием персональных данных.

Управление отклонило жалобу, сочтя, что права субъекта данных не были нарушены и что выдача запросов на доступ к данным в исследовательских целях не входит в компетенцию Управления. В частности, Управление посчитало, что его запрос к контролеру (Управлению начального образования) не является реализацией права на доступ к персональным данным в соответствии со статьей 15 GDPR, а представляет собой запрос на проведение научных исследований.

26 октября 2022 г. субъект данных подал возражение на это решение и запрос на пересмотр дела, в котором утверждал, что его запрос был "не запросом на проведение научного исследования, а личным генеалогическим исследованием, которое далеко от научного исследования, а данные в запрошенном поиске касаются его самого и, таким образом, подпадают под статью 15 GDPR".

Греческий НДПА отклонил запрос на пересмотр. Генеалогическое исследование фамилии не подпадает под действие ст. 15 GDPR как "персональные данные, касающиеся [субъекта данных]". Запрос субъекта данных не являлся запросом на доступ в соответствии со статьей 15 GDPR. Он запросил доступ ко всей базе данных Управления (содержащей персональные данные других субъектов данных), а не доступ к данным, непосредственно относящимся к нему.

## Словенский DPA: видеонаблюдение в туалетах и коридорах не может быть основано на законном интересе

Контроллер считал, что видеонаблюдение было введено для обеспечения защиты имущества и безопасности людей в соответствии с законными интересами контроллера согласно статье 6(1)(f) GDPR. Кроме того, контроллер создал систему безопасности: доступ к архивам видеозаписей защищен паролем, ограничен определенными лицами и возможен только в исключительных случаях, например, для предоставления доказательств в уголовном процессе. Контроллер заявил, что он проинформировал об этом представительный профсоюз и объяснил причины установки камер, которые профсоюз поддержал.

Контроллер также проинформировал своих сотрудников об установке системы видеонаблюдения, разместив информацию об этом на доске объявлений компании. Таким образом, контроллер полагал, что видеонаблюдение соответствует правилам видеонаблюдения, может быть основано на статье 6(1)(f) GDPR.

Камеры видеонаблюдения были установлены таким образом, что охватывали практически все помещения контроллера, включая внешние зоны и ваннные комнаты, где имуществу или людям не может угрожать опасность, не нуждаются в защите.

DPA Словении (Informacijski rooblaščenec) 24.05.2023 предписал контроллеру прекратить использование некоторых видеокамер на территории компании, поскольку видеонаблюдение, например, в туалетах и коридорах, не может быть основано на законном интересе, так как отсутствует реальная угроза имуществу или людям.

Наблюдение за всем помещением только потому, что существует потенциальный риск причинения вреда людям или имуществу, не подпадает под правовые основы ни национального законодательства, ни GDPR. Кроме того, безопасность имущества и людей в определенных местах может быть обеспечена и менее инвазивным способом. В данном случае сотрудники не могли разумно ожидать, что за ними будет вестись видеонаблюдение в уборных и некоторых других помещениях. Таким образом, DPA заявил, что контроллер не выполнил условия теста на законный интерес. Поэтому ПИ пришел к выводу, что контроллер не может ссылаться на статью 6(1)(f) GDPR.

## Австрийский DSB предписал скорректировать баннер cookie и проинформировать сторонних провайдеров об удалении данных заявителя

Посетив 24.09.2021 сайт <https://www.elle.com/> компании Hearst Magazine Media, Inc. (контроллер), заявитель принял cookie-файлы с помощью баннера cookie, на котором отображались только варианты: "принять" или "узнать больше". После этого заявитель обнаружил, что уникальные идентификаторы, позволяющие его идентифицировать, были сохранены на сервере контроллера и затем переданы на серверы сторонних провайдеров, таких как Google и TheTradeDesk.

Австрийский надзорный орган (DSB) счел, что формат cookie-баннера, ранее размещенного на сайте контроллера нарушает GDPR, поскольку в нем отсутствовала опция "отказаться", что является нарушением ст.7(3) GDPR. На этом основании DSB постановил, что заявитель правомерно потребовал удаления своих персональных данных в соответствии со ст.17(1)(d) GDPR, поскольку обработка его персональных данных была незаконной, что также обязывает контроллера уведомить об удалении персональных данных сторонних поставщиков. DSB обязал контроллера проинформировать получателей персональных данных заявителя (в частности, Google и TheTradeDesk) об удалении относящихся к нему данных в соответствии со ст.19 GDPR.

В то же время контроллер изменил баннер cookie-файлов таким образом, чтобы на нем была видна опция "отказ". DSB постановил, что поскольку опция "отклонить" визуально отличается от опции "принять" по цвету и формату, это не является основанием для законного согласия в соответствии со ст.4(11) GDPR. Кроме того, отсутствует четкое указание на то, каким образом можно отозвать свое согласие, поскольку это можно сделать только в конце веб-страницы в разделе "Выбор файлов cookie". Контроллер ошибочно отнес аналитические файлы cookie к категории строго необходимых. Соответственно, DSB предписал контроллеру в течение 8 недель с момента принятия решения адаптировать баннер cookie таким образом, чтобы он соответствовал GDPR.

## Бельгийский APD: соглашение об обработке данных не может применяться задним числом



Бельгийский надзорный орган (APD) отметил, что ст.28(1) GDPR обязывает обработчика предоставлять достаточные гарантии для защиты прав субъектов данных. Ст.28(3) GDPR обязывает контролеров заключать соглашение об обработке данных (DPA). Включение в соглашение оговорки о ретроактивности не исправляет отсутствие договора на момент события. Такой допуск позволил бы обойти применение обязательств ст.28(3) GDPR, направленных на обеспечение защиты прав и свобод субъектов данных. APD пришел к выводу, что как контроллер, так и обработчик несут ответственность за своевременное заключение соглашения об обработке данных.

## Бельгийский APD отклонил жалобы на Google по поводу исключения из поисковой выдачи ссылок на журналистские материалы



Бельгийский надзорный орган (APD) 04.10.2023 отклонил запрос на удаление данных, поданный физическим лицом против компании Google LLC. Ранее были получены четыре различных жалобы от одного и того же физического лица в связи с отказом компании Google исключить ссылки из результатов выдачи поисковой системы Google.

Проведя расследование, APD пришел к выводу, что:

- заявитель играл и продолжает играть роль в общественной жизни;
- содержание ссылок связано с фактами, относящимися к профессиональной деятельности заявителя, и касается вопросов, представляющих важный общий интерес спорный контент был обработан в журналистских целях и получен из надежных журналистских источников;
- информация не является явно недостоверной;
- факты, описанные в спорном материале, являются относительно недавними.

## Временная блокировка обработки данных на платформе ChatGPT из-за отсутствия прозрачности обработки данных



**Кто:** Garante per la protezione dei dati personali (Италия)

**Кого:** OpenAI

**Когда:** 2023.03

**За что:** нарушение ст. 5, 6, 8, 13, 25 GDPR

**Как:** временное ограничение обработки персональных данных итальянцев в чат-боте ChatGPT + 20 дней на устранение выявленных нарушений

**Причина:** отсутствие информации для пользователей и всех заинтересованных сторон, чьи данные собирает OpenAI, а также отсутствие правовой основы для массового сбора и хранения персональных данных с целью "обучения" алгоритмов, лежащих в основе работы платформы.

Регулятор также обращает внимание на то, что сервис, предназначенный для лиц старше 13 лет, не располагает фильтром для проверки возраста пользователей.

Работа чат-бота ChatGPT американской компании OpenAI возобновлена в Италии спустя месяц после блокировки местными властями. Возобновление работы состоялось после того, как OpenAI "прояснила и дала ответ" на те вопросы, которые возникли к ней у итальянского ведомства по защите персональных данных. В компании добавили, что отныне будут лучше информировать пользователей об условиях пользования чат-ботом.



## Выговор оператору цифровой платформы, пользователи которой могли просматривать персональные данные в исходном коде



**DATATILSYNET**

### Databehandler får kritik for manglende sikkerhed

Dato: 28-09-2023

Afgørelse Private virksomheder Kritik Tilsyn / egedriftssag

Anmeldelse af brud på persondatasikkerheden

Datatilsynet har udtalt kritik i en sag, hvor en databehandler, Mindworking A/S, ikke havde sikret passende sikkerhed ved udviklingen af en platform (en webapplikation), der var målrettet ejendomsmæglere.

Journalnummer: 2021-431-0163.

#### Afgørelse

Datatilsynet vender hermed tilbage til sagen, hvor Mindworking A/S (herefter benævnt som Mindworking) den 11. november 2021 som databehandler og leverandør af en platform for en række dataansvarlige har anmeldt et brud på persondatasikkerheden til Datatilsynet. Mindworking anmeldte bruddet på persondatasikkerheden efter en dialog med tilsynet, idet tilsynet i en periode havde modtaget en række anmeldelser om brud på persondatasikkerheden fra ejendomsmæglere, som havde benyttet den platform, som Mindworking havde udviklet. Datatilsynet valgte på den baggrund at undersøge den rejste problemstilling nærmere og indledte en sag mod Mindworking.

Mindworking og Datatilsynet har desuden været i dialog både mundtligt og skriftligt, senest ved Mindworkings besvarelse af tilsynets haring den 22. maj 2023.

Датская компания Mindworking A/S предлагает цифровую платформу "все-в-одном" для сферы недвижимости, выступая в качестве процессора. 04.11.2021 агент по недвижимости уведомил эту компанию о недостатке безопасности в платформе (возникшем еще в момент запуска платформы в 2019 году), о котором стало известно благодаря анонимному сообщению одного из клиентов.

Через инструменты разработчика пользователи могли просматривать конфиденциальные данные в исходном коде веб-страницы, включая личные данные, такие как личные заметки агентов по недвижимости, имена потенциальных покупателей, ценовые предложения и договоры. Разработчик не исключил, что некоторые документы содержали номера социального страхования. Однако чтобы получить доступ к этим данным, пользователи должны были создать учетную запись, войти в платформу и получить доступ к конкретному делу.

Mindworking A/S расследовал ошибку и устранил ее в тот же день, 04.11.2021. Он заявил, что инцидент был вызван ошибкой безопасности, о которой он не знал, поэтому не были приняты технические или организационные меры для предотвращения этой проблемы.

Датский надзорный орган (Datatilsynet) вынес выговор процессору за нарушение статьи 32(1) GDPR. Процессор не обеспечил должной безопасности своей платформы, так как пользователи могли просматривать персональные данные в исходном коде, просто зайдя в инструменты разработчика браузера.

## 1034 Дания: выговор больнице за публикацию фото пациентов на основании их согласий



**DATATILSYNET** HVAD SIGER REGLERNE? ▾

### Hospital kan ikke bruge samtykke til at offentliggøre billeder af patienter på Instagram

Dato: 27-11-2023

Afgørelse Offentlige myndigheder Alvorlig kritik Påbud Tilsyn / egendriftssag

Behandlingsgrundlag Billeder og video Behandlet af Datarådet

Datatilsynet har i en egendriftssag vurderet, at Aarhus Universitetshospitals (Region Midtjylland) offentliggørelse af oplysninger om patienter på Instagram ikke kan ske inden for rammerne af de databeskyttelsesretlige regler.

Journalnummer: 2023-432-0016.

#### 1. Indledende bemærkninger

Datatilsynet vender hermed tilbage til sagen, hvor tilsynet den 19. december 2022 indledte en undersøgelse af egen drift af Aarhus Universitetshospitals (AUH) offentliggørelse af billeder af patienter med tilhørende oplysninger om patienternes helbredstilstande på Instagram.

#### 2. Afgørelse og påbud

Datatilsynet finder – efter at sagen har været forelagt Datarådet – at Region Midtjyllands behandling af personoplysninger i forbindelse med offentliggørelse af fotos af patienter på AUH's Instagramkonto ikke er i overensstemmelse med databeskyttelsesforordningens [1] artikel 9, stk. 2, litra a, og artikel 6, stk. 1, litra a, jf. artikel 4, nr. II.

Endvidere finder Datatilsynet, at behandlingen ikke er i overensstemmelse med principperne i databeskyttelsesforordningens artikel 5, stk. 1.

Гражданин Дании обратился в датский надзорный орган с жалобой на публикацию своей фотографии в Instagram-аккаунте больницы Aarhus University Hospital (AUH).

Больница пояснила, что информация на аккаунте публикуется с целью информирования внешнего мира о деятельности и повседневной жизни больницы. Сообщения, содержащие информацию о гражданах, включая пациентов, были опубликованы на основании согласия в соответствии со статьей 6(1)(a) GDPR и статьей 9(2)(a) GDPR. Согласие было получено в письменной форме до публикации сообщения, и его предоставление или отсутствие не повлияло на медицинское обслуживание, предложенное пациенту.

Надзорный орган постановил нарушение статьи 6(1)(a) и статьи 9(2)(a) GDPR, а также заявил, что обработка данных не могла быть основана на согласии, поскольку из-за асимметрии полномочий между пациентами и больницей пациенты не могли дать свое согласие свободно.

Надзорный орган вынес больнице выговор и в соответствии со статьей 58(2)(d) GDPR обязал больницу удалить посты, содержащие медицинскую информацию о пациентах, из аккаунта в Instagram в течение четырех недель со дня принятия решения.

## 1035 Мальта: предписание добавить метатег no-index в HTML-заголовок статьи онлайн-журнала

Субъект данных обратился в DPA Мальты с просьбой обязать медиакомпанию (контролера) удалить опубликованную статью с ее веб-сайта. В статье его имя (как руководителя игровой компании в то время) связывалось с организованными преступными синдикатами и последующим лишением игорных компаний лицензий на букмекерскую деятельность. Это означало, что при поиске людей по таким словам, как "мафия", "мафиози" или "азартные игры", его имя, скорее всего, будет выведено на экран.

Контролер ответил на жалобу, заявив в DPA, что данные обрабатывались в журналистских целях. Удаление вышеупомянутой статьи поставит под угрозу право на свободу слова и информации. Кроме того, приостановка лицензий на букмекерскую деятельность была предметом судебных разбирательств на Мальте. В соответствии с национальным законодательством журналистские привилегии распространяются и на освещение судебных дел.

Мальтийский DPA обозначил различие между поисковыми системами, такими как Google, и контролером, медиакомпанией. Демократическое общество требует, чтобы СМИ распространяли информацию, отвечающую общественным интересам. Google является онлайн-поисковиком, который ищет в Интернете ключевые слова, введенные пользователем, и возвращает результаты в виде списка. Поскольку жалоба была подана только на контролера, расследование DPA было строго ограничено им.

DPA предписал медиакомпанию добавить метатег no-index в HTML-заголовок содержания интернет-страницы, посвященной делу. Таким образом, основные права заявителя были соблюдены, поскольку его имя было удалено из индекса поисковых систем, что означало, что его имя больше не будет появляться рядом с соответствующими ключевыми словами, на которые он жаловался. В то же время журналистская свобода контролера была сохранена, поскольку оригинальное содержание статьи осталось неизменным.

## Бельгийский APD признал право на удаление данных из церковных (метрических) книг



Человек, пожелавший выйти из католической церкви, подал жалобу в бельгийский APD после того, как епархия Гента отклонила его просьбу об удалении персональных данных из всех метрических книг католической церкви, включая записи крещений. Епархия Гента утверждала, что церковь не удаляет данные из церковных (метрических) книг, а добавляет на полях примечание, отражающее желание человека покинуть церковь. Епархия Гента также утверждала, что церковные (метрические) книги имеют историческую ценность.

Бельгийское управление по защите данных (APD) 19.12.2023 предписало епархии Гента удовлетворить просьбу крещеного человека об удалении данных из церковных (метрических) книг, так как обработка персональных данных заявителя нарушает статьи 5(1)(a), 6(1)(f) и 9 GDPR. Хотя Епархия Гента и ссылалась на законные интересы при обработке персональных данных, она не прошла проверку на необходимость и взвешивание интересов при столкновении с интересами, фундаментальными правами и свободами субъекта данных. Таким образом, обработка данных не подходит для достижения намеченного интереса и не отвечает требованиям ограничения целей и минимизации данных, предусмотренным статьями 5(1)(b) и 5(1)(c) GDPR. Обработка данных на основании канонического права не является основанием для уклонения от выполнения обязательств, предусмотренных GDPR.

## Исландский Persónuvernd предписал удалить пост в социальной сети с данными об уголовном деле



◇ Исландский пользователь Facebook в 2021г. опубликовал фотографии и полицейские отчеты, являвшиеся частью материалов расследования уголовного дела, включая конфиденциальные данные о субъекте данных, в посте на своей странице в Facebook, в котором он высказал свое мнение по этому делу.

◇ Субъект данных, который был жертвой или свидетелем по уголовному делу, подал жалобу в исландский надзорный орган (Persónuvernd). В ответ пользователь Facebook указал, что он не обрабатывал персональные данные субъекта данных, поскольку просто выразил свое мнение по делу, что подпадает под фундаментальную свободу выражения мнения.

◇ Надзорный орган посчитал, что не обладает компетенцией принимать решения по делам, связанным со свободой выражения мнения, но признал применимость GDPR, поскольку пост был доступен всем пользователям Facebook и не являлся обработкой в личных целях. Persónuvernd квалифицировал автора поста как контролера данных в соответствии со ст.4(7) GDPR. Поскольку контролер не был участником уголовного расследования и не должен был получать доступ к полицейским файлам, надзорный орган признал такую обработку данных незаконной в соответствии со ст.6(1)(f) GDPR и предписал автору удалить пост со своей страницы в течение месяца.

## Финский надзорный орган объявил выговор крупнейшему ритейлеру в связи с программой лояльности

◇ Финский надзорный орган Tietosuojavaltuutetun toimisto попросило Kesko Oyj (крупнейшая розничная сеть Финляндии) как контролера объяснить, как он обрабатывает и хранит персональные данные в рамках с программой лояльности.

◇ Контролер пояснил, что обрабатывает основную информацию о клиентах, такую как имя и контактная информация, а также данные о покупательском поведении. Данные о покупательском поведении указывают на подробные данные о покупках клиентов, относящиеся к конкретному продукту. В зависимости от ситуации, информация, связанная с клиентом, стирается в конце отношений с клиентом или анонимизируется не позднее чем через 25 месяцев после окончания отношений с клиентом.

◇ Обработка данных о покупках происходит для развития бизнеса, предоставления льгот и услуг, а также для реализации и таргетирования маркетинга. Контролер подчеркнул, что необоснованное запрещение или ограничение сбора и обработки данных, которые приносят пользу клиенту, подорвет инновации и разработку продуктов, основанные на данных.

◇ Надзорный орган посчитал, что привязка срока хранения данных о покупках к продолжительности отношений с клиентом привела к тому, что данные хранятся в форме, позволяющей идентифицировать субъекта данных в течение потенциально очень длительных периодов, даже десятилетий, что может привести к очень длительному хранению данных о покупках, даже в течение всей жизни субъекта данных. Более того, некоторые из данных о покупках могут быть использованы для получения подробной информации о жизненной ситуации, образе жизни и передвижениях человека. Данные о покупках также могут косвенно раскрывать персональные данные, относящиеся к специальным категориям персональных данных в соответствии со статьей 9 GDPR. Например, клиенты имели возможность накапливать баллы лояльности, пользуясь определенными медицинскими услугами. Риск, связанный с обработкой таких данных, возрастает тем больше, чем более обширные данные собираются и чем дольше они хранятся.

◇ Контролер должен был определить срок хранения данных о покупках с учетом конкретной цели и оценить его отдельно от срока хранения других персональных данных, необходимых для управления отношениями с клиентами. Надзорный орган постановил, что контролер нарушил статьи 5(1)(e), 25(1) и 25(2) GDPR, так как срок хранения данных о покупке, связанный с продолжительностью отношений с клиентом, не был необходим для целей, для которых контролер обрабатывал персональные данные. Кроме того, в соответствии с принципом защиты данных по умолчанию контролер должен был обеспечить субъекту данных возможность с самого начала влиять на уровень сбора своих персональных данных, например, выбрав в регистрационной форме желаемый уровень сбора данных.

## Итальянский надзорный орган заподозрил Sora в угрозе безопасности персональных данных



**Intelligenza artificiale, il Garante privacy avvia istruttoria su "Sora" di OpenAI. Chieste alla società informazioni su algoritmo che crea brevi video da poche righe di testo**

  
- English version

**Intelligenza artificiale, il Garante privacy avvia istruttoria su "Sora" di OpenAI. Chieste alla società informazioni su algoritmo che crea brevi video da poche righe di testo**

Il Garante Privacy ha avviato una istruttoria nei confronti di OpenAI, la società statunitense che nelle scorse settimane ha annunciato il lancio di un nuovo modello di Intelligenza artificiale, denominato "Sora", in grado, da quanto annunciato, di creare scene dinamiche, realistiche e fantasiose, partendo da poche istruzioni testuali.

Considerate le possibili implicazioni che il servizio "Sora" potrebbe avere sul trattamento dei dati personali degli utenti che si trovano nell'Unione europea e in particolare in Italia, l'Autorità ha chiesto ad OpenAI di fornire una serie di chiarimenti.

Entro 20 giorni, la società dovrà precisare se il nuovo modello di intelligenza artificiale sia un servizio già disponibile al pubblico e se venga o verrà offerto ad utenti che si trovano nell'Unione Europea, in particolare in Italia.

OpenAI inoltre dovrà chiarire al Garante una serie di elementi: le modalità di addestramento dell'algoritmo; i dati raccolti ed elaborati per addestrarlo, specialmente se si tratti di dati personali; se tra questi vi siano anche particolari categorie di dati (convinzioni religiose, filosofiche, opinioni politiche, dati genetici, salute, vita sessuale); quali siano le fonti utilizzate.

Nel caso in cui il servizio venga o verrà offerto a utenti che si trovano nell'Ue, il Garante ha chiesto in particolare alla società di indicare se le modalità previste per informare utenti e non utenti e le basi giuridiche del trattamento dei dati forniti di quanti accedono al servizio siano conformi al Regolamento europeo.

Roma, 8 marzo 2024

---



**Artificial intelligence: the Italian Data Protection Authority opens an investigation into OpenAI's 'Sora'**  
OpenAI asked to provide information on the algorithm that creates short videos from text instructions

Управление по защите данных Италии (Garante) начало расследование в отношении новой модели искусственного интеллекта (ИИ) от американской корпорации OpenAI Sora – нейросети, которая генерирует видеоролики по текстовому описанию.

Garante предоставила OpenAI 20 дней на подготовку ответов на уточняющие вопросы:

- как обучается Sora, какие данные собираются и обрабатываются для обучения нейросети;
- собирает ли сервис конфиденциальную информацию;
- какие источники использует Sora для сбора сведений.

Garante намерена выяснить потенциальные последствия, которые Sora может иметь для обработки персональных данных пользователей в Евросоюзе и, в частности, в Италии.

Также Garante запросила разъяснения относительно того, какие методы будет использовать сервис для информирования пользователей об обработке персданных и правовых основаниях для обработки в соответствии с законодательством ЕС.

## В Испании и Португалии временно запретили работу криптопроекта Worldcoin с биометрией для защиты данных пользователей



◇ Испанское агентство по защите данных (AEPD) потребовало от корпорации Tools for Humanity прекратить сбор и обработку некоторых категорий персональных данных. Tools for Humanity уже заблокировала собранные данные.

◇ Обработка биометрических данных согласно GDPR заслуживает особой защиты из-за их конфиденциального характера. В связи с этим регулятор принял временные меры, направленные на немедленное прекращение обработки таких данных и их возможной передачи третьим лицам.

◇ У Tools for Humanity есть европейское представительство в Германии. Меры в отношении компании ввели на три месяца, пока она не устранил нарушения.

◇ В июле 2023 года гендиректор OpenAI Сэм Альтман запустил криптовалютный проект Worldcoin, в котором используются биометрические данные для аутентификации. В рамках проекта счёт World ID сможет открыть только реальный человек. Чтобы получить World ID, он должен зарегистрироваться и пройти процедуру сканирования радужной сетчатки глаза при личной встрече с помощью «сферы» Worldcoin. После завершения сканирования человек добавляется в базу данных, а Worldcoin создает уникальный криптографический «хэш». Данные сканирования не сохраняются, но хэш можно использовать в будущем для анонимного подтверждения личности через приложение, которое включает закрытый ключ, связанный с общедоступным открытым ключом.


◇ Португальский орган по защите данных (CNPd) опубликовал 26.03.2024 временно (90 дней) запретило Worldcoin сбор биометрии.

<https://www.aepd.es/en/press-and-communication/press-releases/agency-orders-precautionary-measure-which-prevents-Worldcoin-from-continuing-to-process-personal-data-in-spain>

<https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/123142>



## Испания: слово "небинарный" в ответе на вопрос анкеты о половой принадлежности является обработкой специальной категории

		1/26
<p>• Expediente N.º: EXP202202954</p>		
ANTECEDENTES.....		2
PRIMERO.....		2
SEGUNDO.....		2
TERCERO.....		2
CUARTO.....		2
QUINTO.....		6
SEXTO.....		6
SEPTIMO.....		6
OCTAVO.....		7
HECHOS PROBADOS.....		7
PRIMERO.....		7
SEGUNDO.....		7
TERCERO.....		7
CUARTO.....		7
QUINTO.....		7
SEXTO.....		8
FUNDAMENTOS DE DERECHO.....		8
Competencia.....		8
Normativa aplicable.....		9
Licitud del tratamiento.....		10
Primera obligación incumplida: infracción del artículo 5.1.c) del RGPD.....		13
Tipificación de la infracción del artículo 5.1.c) del RGPD.....		16
Segunda obligación incumplida: infracción del artículo 9.1 del RGPD.....		17
Tipificación de la infracción del artículo 9.1 RGPD.....		21
Régimen aplicable a las Administraciones Públicas.....		22
Medidas correctoras.....		24
RESUELVE.....		24
<p><small>© Jorge Juliá, 6 2000 - Madrid</small></p> <p style="text-align: right;"><small>www.aepd.es www.gdprhub.eu</small></p>		

31.01.2022 в испанское агентство по защите данных (AEPD) была подана жалоба на правительственную веб-страницу, на которой требовалось указать определенные персональные данные, чтобы отправить форму для примирения трудовых споров в Департамент экономики, знаний и занятости Канарских островов (контролер). В частности, в форму был включен вопрос о поле/генде, на который требовалось ответить "мужчина", "женщина" или "небинарный". Субъект данных утверждал, что небинарный ответ требует раскрытия персональных данных, связанных с сексуальной ориентацией, и что такие данные выходят за рамки правовой основы контролера и цели формы.

AEPD определил, что контролер обрабатывал специальные категории информации, что запрещено ст.9(1) GDPR. Отметив, что гендерная идентичность и сексуальная ориентация отличаются друг от друга, AEPD определил, что ответ, отличный от мужского или женского (в данном случае небинарный), все равно может считаться относящимся к сексуальной жизни, даже если в форме нет прямой ссылки на сексуальную ориентацию или сексуальную жизнь. В данном случае не было применимого исключения из запрета на обработку специальных категорий в соответствии со ст.9(2) GDPR. В результате AEPD пришел к выводу, что небинарный ответ нарушает статью 9(1) GDPR..

<https://www.aepd.es/documento/ps-00070-2023.pdf>

[https://gdprhub.eu/index.php?title=AEPD\\_\(Spain\)\\_-\\_EXP202202954](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202202954)

## 1042 Расследование работы платформы ChatGPT

- ◇ Европейский совет по защите данных (EDPB) обсудил временный запрет, наложенный итальянским органом по защите данных ("Garante") на компанию OpenAI, L.L.C. в отношении ее сервиса ChatGPT, и [принял решение](#) о создании специальной целевой группы для развития сотрудничества и обмена информацией о возможных правоприменительных действиях, проводимых другими европейскими DPA.
- ◇ Испанское агентство по защите персональных данных (AEPD) инициировало [предварительное расследование](#) в отношении деятельности компании OpenAI — разработчика чат-бота ChatGPT. AEPD объяснило свое решение «возможным нарушением норм». На прошлой неделе ведомство попросило Европейский комитет по защите данных включить этот вопрос в повестку одного из следующих заседаний.
- ◇ Нидерландский орган по защите данных (AP) [потребовал](#) от компании OpenAI, L.L.C. предоставить разъяснения по поводу обработки персональных данных при использовании генеративного искусственного интеллекта (ИИ). В частности, AP подчеркнул свой интерес к тому, как OpenAI обрабатывает персональные данные при обучении ChatGPT.
- ◇ Польше [проверяют](#) деятельность технологической компании OpenAI на предмет нарушения GDPR. «Дело касается нарушения многих положений о защите персональных данных, поэтому мы попросим OpenAI ответить на ряд вопросов», — заявил глава UODO Ян Новак. В управлении добавили, что OpenAI не исправляла ложную информацию, сгенерированной принадлежащей ей нейросетью ChatGPT.
- ◇ Итальянский надзорный орган (Garante) [уведомил](#) OpenAI о том, в действиях компании усматривается нарушение законодательства ЕС о персональных данных. Компании предложено направить свои возражения в течение 30 дней. При вынесении окончательного решения по данному делу Garante примет во внимание итоги расследования специальной рабочей группой EDPB по ChatGPT. Предварительные выводы Garante, что при разработке и эксплуатации ChatGPT компания могла нарушить требования ст. 5, 6, 8, 13 и 25 GDPR:
  - отсутствие законной основы для обработки персональных данных,
  - необеспечение точности обработки,
  - ненадлежащее информирование субъектов персональных данных,
  - необеспечение защиты интересов несовершеннолетних при их доступе к сервису,
  - несоблюдение принципов конструктивной защиты данных и защиты данных по умолчанию.

## 1043 CNIL, ICO, HDPА, DSB уличили Clearview AI в нарушении GDPR

◇ Французский CNIL [предписал](#) компании Clearview AI, предлагающей сервис по распознаванию лиц, прекратить собирать и использовать данные граждан Франции. Набор общедоступных изображений лиц Clearview AI в социальных сетях и интернете не имеет правовой основы и нарушает GDPR. Регулирующий орган заявил, что компания не запросила предварительного согласия людей, чьи изображения были собраны в Сети. Нью-Йоркская фирма не предоставила заинтересованным лицам надлежащий доступ к своим данным, в частности, безосновательно ограничив доступ до двух раз в год, а также ограничив это право данными, накопленными в течение 12 месяцев до подачи любого запроса.


◇ Австрийский DSB [предписал](#) компании Clearview AI удалить ранее собранные данные одного из граждан Австрии и назначить представителя в ЕС

Компания Clearview AI была оштрафована следующими надзорными органами:

◇ британский [ICO](#) – 7,5 млн фунтов;

◇ греческий [HDPА](#) – €20 млн;

◇ французский [CNIL](#) – €20 млн. + €5,2 млн за [невыполнение предписания CNIL](#) от 17.10.2022

 Британский трибунал первой инстанции [посчитал](#), что поднадзорный им орган по защите данных (ICO) не имел компетенции привлечь американскую компанию Clearview AI к ответственности. Трибунал установил, что компания Clearview, хотя сама и не "отслеживает поведение" на подведомственной ICO территории (один из критериев экстерриториального применения EU GDPR и UK GDPR), но предоставляет для этого технические средства своим клиентам, а также определяют цели и средства обработки персональных данных. Трибунал отметил, что по обстоятельствам дела этого было бы достаточно, чтобы признать компанию сооператором обработки персональных данных наряду со её клиентами. Вместе с тем, трибунал посчитал, что сценарий работы Clearview не входит в предмет регулирования GDPR, так как пользователями сервиса биометрической идентификации компании являются только полицейские и спецслужбы иностранных государств (либо их частные подрядчики, но действующие в публичном интересе).

## Судебная практика – базы решений и интересные ситуации




# Обзор судебной практики ECHR по защите персональных данных за 1978-2021 гг.

## European Court of Human Rights

Регулярно актуализируемый обзор судебной практики Европейского суда по правам человека (ECHR), который затрагивает следующие области:

- сбор персональных данных
- хранение и использование персональных данных
- раскрытие персональных данных
- доступ к персональным данным
- стирание или уничтожение персональных данных



Press Unit  
Unité de la Presse

EUROPEAN COURT OF HUMAN RIGHTS  
COUR EUROPÉENNE DES DROITS DE L'HOMME

September 2019  
The factsheet does not bind the Court and is not exhaustive

Factsheet – Personal data protection

## Personal data protection

"The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of **Article 8** [of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence]<sup>1</sup> ... The subsequent use of the stored information has no bearing on that finding ... However, in determining whether the personal information retained by the authorities involves any ... private-life [aspect] ... the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained ..." (*S. and Marper v. the United Kingdom*, judgment [Grand Chamber] of 4 December 2008, § 67)

### Collection of personal data

#### DNA information and fingerprints

See below, under "Storage and use of personal data", "In the context of police and criminal justice".


#### GPS data

[Uzun v. Germany](#)  
2 September 2010

The applicant, suspected of involvement in bomb attacks by a left-wing extremist movement, complained in particular that his surveillance via GPS and the use of the data obtained thereby in the criminal proceedings against him had violated his right to respect for private life.

The Court held that there had been **no violation of Article 8** of the Convention. The GPS surveillance and the processing and use of the data thereby obtained had admittedly interfered with the applicant's right to respect for his private life. However, the Court noted, it had pursued the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime. It had also been proportionate: GPS surveillance had been ordered only after less intrusive methods of investigation had proved insufficient, had been carried out for a relatively short period (some three months), and had affected the applicant only when he was travelling in his accomplice's car. The applicant could not therefore be said to have been subjected to total and comprehensive surveillance. Given that the investigation had concerned very serious crimes, the applicant's surveillance by GPS had thus been necessary in a democratic society.

<sup>1</sup> Article 8 of the [European Convention on Human Rights](#) provides that:  
 "1. Everyone has the right to respect for his private and family life, his home and his correspondence.  
 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."



CONSEIL DE L'EUROPE  
COUNCIL OF EUROPE

# Обзор судебной практики Суда Европейского союза (CJEU) по защите персональных данных



DPcuria.eu  
Data Protection Case Law

[Home](#)

[About](#)

[Content](#)

[Contact & privacy](#)

## Full text search



## Search by category



## Latest preliminary rulings

- 02 Mar 2021: [C-746/18](#) (*Prokuratuur*)
- 11 Nov 2020: [C-61/19](#) (*Orange Romania*)
- 06 Oct 2020: [C-623/17](#) (*Privacy International*)
- 06 Oct 2020: [C-511/18](#) (*La Quadrature du Net and others*)
- 16 Jul 2020: [C-311/18](#) (*Facebook Ireland and Schrems*)
- 09 Jul 2020: [C-272/19](#) (*Land Hessen*)
- 11 Dec 2019: [C-708/18](#) (*Asociatia de Proprietari bloc ...*)
- 01 Oct 2019: [C-673/17](#) (*Planet49*)
- 24 Sep 2019: [C-136/17](#) (*GC and Others*)
- 24 Sep 2019: [C-507/17](#) (*Google*)
- 29 Jul 2019: [C-40/17](#) (*Fashion ID*)
- 14 Feb 2019: [C-345/17](#) (*Buivids*)
- 02 Oct 2018: [C-207/16](#) (*Ministerio Fiscal*)
- 10 Jul 2018: [C-25/17](#) (*Jehovan todistajat*)
- 05 Jun 2018: [C-210/16](#) (*Wirtschaftsakademie Schleswig-...*)
- [More...](#)

## Latest referrals

- 23 Mar 2021: [C-180/21](#) (*Inspektor v Inspektorata kam V...*)
- 09 Mar 2021: [C-154/21](#) (*Österreichische Post*)
- 03 Mar 2021: [C-132/21](#) (*Budapesti Elektromos Művek*)
- 02 Mar 2021: [C-129/21](#) (*Proximus*)
- 08 Feb 2021: [C-77/21](#) (*Digi*)
- 20 Jan 2021: [C-34/21](#) (*Hauptpersonalrat der Lehrerinn...*)
- 22 Dec 2020: [C-701/20](#) (*Avis Autovermietung*)
- 13 Nov 2020: [C-601/20](#) (*SOVIM*)
- 21 Oct 2020: [C-534/20](#) (*Leistritz*)
- 24 Sep 2020: [C-460/20](#) (*Google*)
- 15 Jul 2020: [C-319/20](#) (*Facebook Ireland*)
- 29 May 2020: [C-245/20](#) (*Autoriteit Persoonsgegevens*)
- 28 Apr 2020: [C-184/20](#) (*Vyriausioji tarnybinės etikos...*)
- 14 Apr 2020: [C-175/20](#) (*Valsts ieņēmumu dienests*)
- 31 Oct 2019: [C-817/19](#) (*Ligue des droits humains*)
- [More...](#)



## Court of Justice of the European Union

*Judgment in Case C-210/16*

*Decision on 5 June 2018*

*Wirtschaftsakademie Schleswig-Holstein*

Администратор группы в Facebook совместно с самой социальной сетью является контролером обрабатываемых данных посетителей страницы и несет ответственность за их обработку.

*Judgment in Case C-25/17*

*decision on 10 July 2018*

*Tietosuojaaltuutettu*

Религиозное объединение совместно с членами своих общин является контролером персональных данных, обрабатываемых в ходе проповеднической деятельности «от двери к двери», посредством которой члены общин, участвующие в проповедовании, распространяют веру своей общины. Хотя собранные персональные данные могут не передаваться религиозному объединению, но оно организывает, координирует и поощряет проповедническую деятельность своих общин.

## CJEU о необходимости получать согласия посетителей сайта при размещении на нем социального плагина

### Court of Justice of the European Union

*Judgment in Case C-40/17*

*Decision on 29 July 2019*

*Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*



Recueil de la jurisprudence

ARRET DE LA COUR (deuxième chambre)

29 juillet 2019\*

« Renvoi préjudiciel – Protection des personnes physiques à l'égard du traitement des données à caractère personnel – Directive 95/46/CE – Article 2, sous d) – Notion de "responsable du traitement" – Gestionnaire d'un site Internet ayant incorporé sur celui-ci un module social qui permet la communication des données à caractère personnel du visiteur de ce site au fournisseur dudit module – Article 7, sous f) – Légitimation des traitements de données – Prise en compte de l'intérêt du gestionnaire du site Internet ou de celui du fournisseur du module social – Article 2, sous h), et article 7, sous a) – Consentement de la personne concernée – Article 10 – Information de la personne concernée – Réglementation nationale permettant aux associations de défense des intérêts des consommateurs d'agir en justice »

Dans l'affaire C-40/17,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par l'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf, Allemagne), par décision du 19 janvier 2017, parvenue à la Cour le 26 janvier 2017, dans la procédure

**Fashion ID GmbH & Co. KG**

contre

**Verbraucherzentrale NRW eV,**

en présence de :

**Facebook Ireland Ltd,**

**Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen,**

LA COUR (deuxième chambre),

composée de M. K. Lenaerts, président de la Cour, faisant fonction de président de la deuxième chambre, M<sup>mes</sup> A. Prechal, C. Toader, MM. A. Rosas (rapporteur) et M. Ilesić, juges,

avocat général : M. M. Bobek,

greffier : M. D. Dittert, chef d'unité,

vu la procédure écrite et à la suite de l'audience du 6 septembre 2018,

Владелец сайта Fashion ID и Facebook признаны совместными контролерами в отношении обработки (сбор и разглашение посредством передачи) данных посетителей указанного сайта при размещении на сайте социального плагина FB в виде веб-кнопки «Нравится». На владельца сайта возложена обязанность информирования посетителей сайта о такой обработке их персональных данных и получения согласия посетителей на нее (включая передачу данных в Facebook). Владелец сайта не несет ответственность за дальнейшую обработку полученных Facebook персональных данных посетителей.

Нужно учитывать, что решение было принято на основании положений уже не действующей Directive 95/46/EC, но ценна сама позиция суда и описание ситуации.



# CJEU о хранении cookies и о предварительно отмеченных флажках для выражения согласия на веб-сайтах



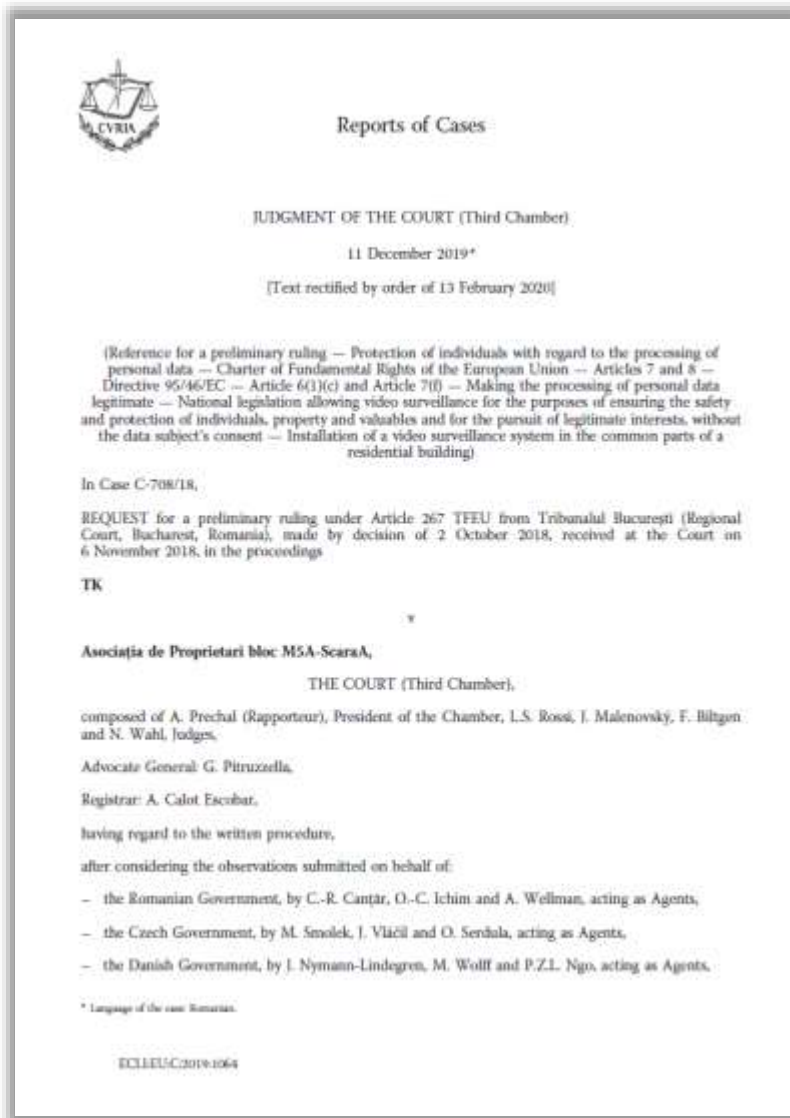
## Court of Justice of the European Union

### *Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände– Verbraucherzentrale Bundesverband eV v Planet49 GmbH*

Решение суда относится к согласиям, собираемым с использование веб-сайтов:

- согласие должно активно выражаться через действия пользователя;
- согласие должно быть понятным и недвусмысленным, описанным в простых словах;
- никаких галочек/флажков/т.п. не должно быть по умолчанию, снятие пользователем заранее поставленной галочки – не активное действие;
- согласие должно содержать описание всех деталей обработки (цель, категории, действия и т.д.);
- для cookies указываются период (срок, условие) их обработки, а также сведения о доступе к ним третьих лиц с указанием категорий таких лиц.

## CJEU об использовании CCTV на основании законного интереса контролера



## Court of Justice of the European Union

### *Judgment in Case Case C-708/18 TK v Asociația de Proprietari bloc M5A-Scara A*

Решение суда относится к отдельно взятому случаю в Румынии:

- система видеонаблюдения (CCTV) была установлена в общедоступной зоне жилого комплекса в целях обеспечения физической безопасности жильцов и посетителей;
- местное законодательство Румынии запрещает использование CCTV без согласия субъекта на обработку данных в целях предотвращения преступности и обеспечения защиты людей и имущества;
- CJEU посчитал, что использование CCTV в данной конкретной ситуации возможно на основании ст.6(1)(f) GDPR;
- в своём решении суд учитывал наличие в прошлом случаев вандализма и взломов, которые имели место быть, несмотря на установленную в жилом комплексе СКУД.



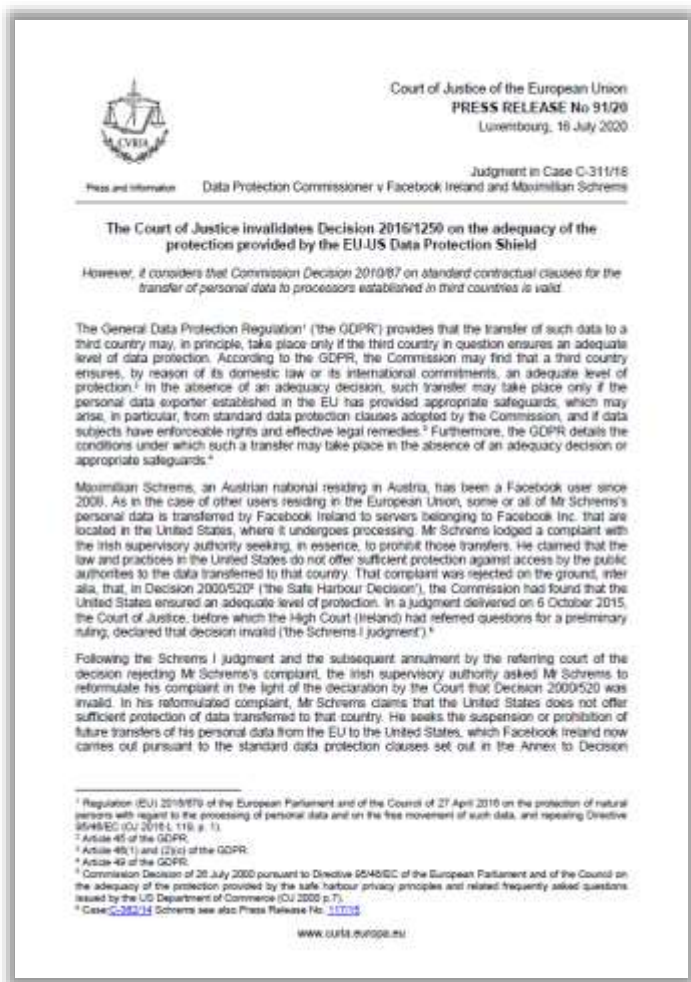
## Court of Justice of the European Union

### *Judgment in Case Constantin Film Verleih GmbH v. YouTube LLC and Google Inc. (C-264/19)*

Суд постановил, что YouTube в соответствии с Directive 2004/48/EC on the Enforcement of Intellectual Property Rights не обязан передавать адреса электронной почты, номера телефонов и IP-адреса пользователей, которые незаконно загрузили фильмы Scary Movie 5 и Parker на видеоплатформу в 2013 и 2014 годах. Запрос о предоставлении указанных данных исходил от компании, которая имела права на распространение этих фильмов в Германии.

По мнению суда необходимо соблюдать баланс между защитой персональных данных и авторским правом. Само дело было передано в CJEU после того, как немецкий суд запросил дополнительные разъяснения о том, что должны делать видеоплатформы для борьбы с пиратством фильмов.

# CJEU о недействительности Privacy Shield и об уточнении в отношении стандартных договорных условий (SCC-P)



## Court of Justice of the European Union

*Judgment in Case C-673/17*

*Data Protection Commissioner v*

*Facebook Ireland Limited, Maximilian Schrems*

Суд постановил, что:

1. Privacy Shield признается недействительным в связи с недостаточной защищенностью персональных данных от передачи операторами социальных сетей американским спецслужбам. В решении суда говорится, что данное соглашение создает условия для нарушения фундаментальных прав европейских граждан. В нем подчеркивается, что в США доступ государственных структур к подобной информации ограничен в гораздо меньшей степени, чем в странах ЕС.

2. SCC-P (Standard Contractual Clauses Controller-to-Processor) не должны быть признаны недействительными, но экспортеры и импортеры персональных данных из ЕС должны предпринимать необходимые и достаточные меры для обеспечения соблюдения SCC-P. В частности, экспортер данных при содействии импортера должен оценить адекватность защиты прав субъектов данных в юрисдикции импортера данных, а также способен ли импортер данных выполнять все требования SCC-P. Кроме того, надзорные органы ЕС (DPA) обязаны приостановить или запретить передачу данных в третью страну, если они считают принципиально невозможным обеспечение требуемого законодательством ЕС уровня защиты прав субъектов данных, даже при наличии действующего SCC между экспортером и импортером.

# CJEU об использовании данных о местоположении в контексте расследований преступлений



## Court of Justice of the European Union

### *Judgment in Case C-746/18 H. K. v Prokuratuur*

Суд постановил, что доступ к данным о местонахождении, полученным из электронных сообщений, может быть использован только правоохранительными органами при расследовании тяжких преступлений и для «предотвращения серьезных угроз общественной безопасности». CJEU установил, что закон ЕС имеет приоритет над национальным законодательством, которое дает прокуратуре право разрешать доступ к таким данным в ходе уголовного расследования.



**Court of Justice of the European Union**  
*Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others*

Суд постановил, что безудержное массовое наблюдение за телефонными и интернет-данными является незаконным, что необходимо ограничить полномочия спецслужб во Франции и других странах ЕС. Суд ЕС заявил, что общее и неизбирательное хранение таких данных может быть разрешено только тогда, когда правительства сталкиваются с «серьезной угрозой национальной безопасности». В такой ситуации полный доступ к данным пользователей телефона и Интернета должен быть ограничен периодом, который «строго необходим», говорится в заявлении суда.

Постановление высшего суда ЕС также разрешило сбор и хранение IP-адресов в тех же пределах, когда это «строго необходимо». Суд ЕС заявил, что национальные суды не должны принимать во внимание информацию, собранную властями, которые не соблюдают принципы, изложенные в данном постановлении CJEU.

# CJEU о неприемлемости всеобщего и неизбирательного хранения сотовых данных в ЕС



## Court of Justice of the European Union

*Judgment in Case C-140/20*

*Commissioner of An Garda Síochána and others*

Суд вынес решение по делу, возбужденному Верховным судом Ирландии, в котором человек, приговоренный в 2015 году к пожизненному заключению за убийство, подал апелляцию, заявив, что суд первой инстанции ошибочно принял данные о трафике телефонных звонков и местоположении пользовательского устройства в качестве доказательства.

CJEU постановил, что национальный суд должен оценить допустимость таких доказательств, и отметил, что государства-члены ЕС не могут иметь законы, которые позволяли бы предотвращать преступления путем «всеобщего и неизбирательного» хранения таких данных.



## Court of Justice of the European Union

*Judgment in Case C-61/19*

*Orange România SA v*

*Autoritatea Națională de Supraveghere a Prelucrării Datelor cu*

*Caracter Personal (ANSPDCP)*

Суд вынес решение по делу между Национальным органом по надзору за обработкой персональных данных Румынии (ANSPDCP) и телекоммуникационным оператором Orange România. ANSPDCP наложил штраф на том основании, что Orange România копировала документы, удостоверяющие личность клиента, и хранила их без согласия. CJEU указал, что клиенты телекоммуникационной компании не давали своего свободного, конкретного и осознанного согласия на осуществление таких действий при заключении договора с Orange România.

Клиентам не было очевидно, что отказ от копирования и хранения их идентификационных документов не делает невозможным заключение договора. Иначе говоря, субъекты не имели возможности сделать осознанный выбор, если не имели представления о его последствиях

Также было отмечено, что не является добросовестной практикой со стороны компании требование к своим клиентам подкреплять свой отказ от копирования и хранения копий удостоверяющих личность документов в виде письменного заявления. Для предоставления согласия требуется положительное действие субъекта данных, а в рассматриваемом случае возникает обратная ситуация: необходимы позитивные действия, чтобы отказаться от согласия (по аналогии с делом Planet49, где снятие галочки с предварительно отмеченного чекбокса на веб-сайте считается слишком большим бременем для пользователя, то нельзя ожидать, что клиент тем временем откажется от своего согласия в рукописной форме).



# CJEU о несовместимости публичного реестра нарушений правил дорожного движения Латвии с GDPR



## Court of Justice of the European Union

### *Judgment in Case C-439/19 Latvijas Republikas Saeima*

22.06.2021 суд вынес решение в документе о несовместимости с GDPR Закона Латвии о дорожном движении от 01.10.1997 («Закон о дорожном движении»), который требует от Управления безопасности дорожного движения Латвии (CSDD) вести публичный реестр, содержащий данные, касающиеся штрафных баллов, наложенных на водителей за нарушение правил дорожного движения. В частности, CSDD может раскрыть такую информацию любому лицу, которое запросит, без необходимости устанавливать конкретный интерес в получении этой информации, независимо от коммерческих или некоммерческих мотивов.

Суд отметил, что информация, касающаяся штрафных баллов, представляет собой персональные данные и что деятельность, связанная с безопасностью дорожного движения, не может быть классифицирована как имеющая целью обеспечение национальной безопасности и, таким образом, подпадает под действие GDPR. CJEU признал, что повышение безопасности дорожного движения рассматривается как отвечающее общественным интересам, но для этого существуют менее навязчивые средства и что в свете конфиденциальности персональных данных права субъектов преобладают над общественными интересами и правом на свободу информации.



## Court of Justice of the European Union

### *Judgment in Case C-645/19 Facebook Ireland and Others*

15.06.2021 суд уточнил условия осуществления полномочий национальных надзорных органов в отношении трансграничной обработки данных. При определенных условиях национальный надзорный орган может воспользоваться своими полномочиями для возбуждения расследования по любому предполагаемому нарушению GDPR в суде государства-члена ЕС, даже если этот орган не является ведущим надзорным органом в отношении этой обработки.

До сих пор на такие иски отвечал ПД-регулятор Ирландии, поскольку европейские штаб-квартиры Microsoft, Intel, Facebook, Google, Apple, Twitter и пр. американских IT-компаний располагались там. Теперь исков к этим компаниям по поводу нарушений законодательства о ПД станет больше, отмечает издание, а регулирование в их отношении – строже. Ирландию давно обвиняли в том, что она медлит с распространением требований GDPR (введённых в 2018 году) на американских IT-гигантов, а также облагает их слишком низким налогом.

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62019CA0645&rid=8>

<https://d-russia.ru/evropejskij-sud-lishil-irlandiju-prava-predstavljat-interesy-vseh-stran-es-v-kachestve-reguljatora-v-oblasti-pd.html>



## Court of Justice of the European Union

### *Judgment in Case C-319/20 Meta Platforms Ireland*

28.04.2022 суд постановил, что ассоциации по защите прав потребителей (в контексте спора с Meta Platforms Ireland) могут инициировать разбирательства в отношении лиц, предположительно ответственных за нарушение законодательства, гарантирующего защиту персональных данных, даже будучи не уполномоченными. Ранее Facebook Ireland была обвинена в нарушении немецкого законодательства о защите персональных данных, что равносильно недобросовестной коммерческой практике, нарушению закона о защите прав потребителей и нарушению запрета на использование недействительных общих условий.

# CJEU признал сведения, косвенно раскрывающие сексуальную ориентацию, чувствительными персональными данными



## Court of Justice of the European Union

Judgment in Case C-184/20

OT v Vyriausioji tarnybinės etikos komisija

01.08.2022 суд разъяснил понятие «особая категория персональных данных» и дал широкую трактовку этому понятию. Ст.9(1) GDPR предусматривает, что запрещается обработка персональных данных, «раскрывающих» расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, членство в профсоюзе, а также обработка данных, «касающихся» здоровья или данных, «касающихся» сексуальной жизни или сексуальной ориентации физического лица.

Глагол «раскрывать» соответствует принятию во внимание обработки не только изначально чувствительных данных, но и данных, раскрывающих информацию такого характера косвенно, после интеллектуальной операции, включающей дедукцию или перекрестные ссылки, а предлог «касающийся», напротив, означает наличие более прямой и непосредственной связи между обработкой и соответствующими данными, рассматриваемыми как изначально чувствительные.

Эти положения не могут быть истолкованы как означающие, что обработка данных, которые косвенно могут раскрыть чувствительную информацию о физическом лице, исключается из режима усиленной защиты, предписанного этими положениями, если эффективность этого режима и защита основных прав и свобод физических лиц, которые он призван обеспечить, не должны быть поставлены под угрозу.

Ст.9(1) GDPR должна быть истолкована как означающая, что публикация данных, которые могут косвенно раскрыть сексуальную ориентацию физического лица, представляет собой обработку специальных категорий персональных данных в целях этих положений.

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=263721>

<https://techcrunch-com.cdn.ampproject.org/c/s/techcrunch.com/2022/08/02/cjeu-sensitive-data-case/amp/>

# CJEU назвал незаконным сбор личных данных всех граждан ЕС в антитеррористических целях



## Court of Justice of the European Union

*Judgment in Case C-793/19*

*Bundesrepublik Deutschland v SpaceNet AG*

Суд ЕС назвал незаконным раздел разработанного Еврокомиссией антитеррористического законодательства Евросоюза, которое обязывает мобильных операторов хранить базы данных по переговорам и коммуникациям всех граждан ЕС в течение трех лет. Об этом говорится в вердикте Европейского суда юстиции, вынесенном во вторник в Люксембурге.

"Суд юстиции постановил, что нормы ЕС исключают общий и нецелевой сбор и хранение данных о мобильном трафике и геолокации [граждан], за исключением случаев, когда есть серьезная угроза национальной безопасности", - отмечается в постановлении.

Иск против германского государства, обязавшего своих мобильных операторов собирать и хранить базы данных по всем переговорам граждан в течение как минимум трех лет, подали мобильный оператор Deutsche Telekom и провайдер мобильной связи SpaceNet AG. Между тем, оспариваемый ими германский закон является лишь отражением директивы ЕС о сборе персональных данных в целях безопасности в законодательстве ФРГ.

Данная директива была принята в 2017 году на волне крупных терактов, совершенных радикальными исламистами во Франции, Бельгии и Великобритании в 2015-2016 годах. Еврокомиссия рассматривает создание провайдерами интернет-услуг закрытых баз данных всех видов электронной коммуникации всех пользователей европейского сегмента Интернета важным подспорьем, которое может использоваться спецслужбами для борьбы с терроризмом.

# CJEU о последствиях отзыва согласия на обработку данных и об уведомлении получателей данных



## Court of Justice of the European Union

### Judgment in Case C-129/21

#### *Proximus NV v Gegevensbeschermingsautoriteit*

Суд ЕС указал, что контролеры должны принимать разумные меры для передачи запросов субъектов данных другим контролерам в цепочке поставок, обрабатывающим те же данные. Неспособность сделать это может привести к тому, что все контролеры будут незаконно обрабатывать персональные данные. Из этого следует, что контролеры должны соответствующим образом проверять все потоки данных в таких цепочках поставок, чтобы убедиться, что они соблюдают свои общие обязательства по подотчетности и что их обработка данных соответствует GDPR.

Отзыв согласия на обработку данных субъектом данных, как это предусмотрено ст.12 Директивы 2002/58/ЕС (ePrivacy Directive), включает в себя запрос на удаление данных в соответствии со ст.17 GDPR, поэтому контроллеры должны убедиться, что в случае, когда субъект данных требует удаления своих персональных данных, контроллер действительно удаляет данные, а не просто изменяет их категорию.

Если не указано иное, отзыв согласия субъекта данных требует удаления только тех данных, которые являются предметом конкретной обработки. Это было важно в данном случае, поскольку компания Proximus утверждала, что любой отзыв согласия потребует как от нее, так и от компании Telenet (которая собирала первоначальное согласие и имела отдельные договорные отношения с заявителем на предоставление телекоммуникационных услуг) удалить данные заявителя из всех своих баз данных, что сделает невозможным выполнение контракта Telenet с заявителем.

# CJEU разъяснил условия обеспечения "права на забвение" в деле против Google



## Court of Justice of the European Union

### *Judgment in Case C-460/20*

Суд ЕС вынес решение по делу о якобы неправомерном отказе компании Google удалить ссылки на предположительно неверную информацию по поисковой выдаче имен двух менеджеров инвестиционной фирмы, за разъяснениями по которому к нему обратился Федеральный суд ФРГ.

Менеджеры настаивали, что информация, получаемая по поиску Google в сети Интернет на основе их имен, в частности, содержит отсылки к двум статьям, несправедливо, по их мнению, критикующим инвестиционную модель группы компаний, работниками которой они являлись, поскольку эта критика якобы опиралась на неверные утверждения.

Google, в свою очередь, утверждала, что отказ в осуществлении «права на забвение» основывался на невозможности с ее стороны самостоятельно определить степень достоверности или ложности информации, затребованной к удалению, в связи с ее профессиональным характером.

Право на защиту персональных данных не является абсолютным, и при его осуществление учитываться должны также функции такой информации в обществе, то есть, должен соблюдаться баланс осуществления иных фундаментальных прав на основе принципа пропорциональности.

В случае, если лицо, обращающееся с требованием об удалении каких-либо сведений из выдачи результатов поиска в сети Интернет, предоставляет относящиеся к делу и достаточные доказательства своего «права на забвение», оператор поисковой системы обязан удовлетворить такое требование, особенно в случае, если таковое подтверждается соответствующим судебным решением.

<https://curia.europa.eu/juris/liste.jsf?num=C-460/20>

[https://www.rapsinews.ru/international\\_news/20221208/308547763.html](https://www.rapsinews.ru/international_news/20221208/308547763.html)



## Court of Justice of the European Union

### *Judgment in Joined Cases C-37/20 and C-601/20 Sovim*

Суд ЕС признал незаконным ключевое положение Директивы ЕС об отмывании средств, полученных преступным путем, согласно которому информация о бенефициарных владельцах, зарегистрированных в европейских национальных «реестрах прозрачности», была общедоступной. Таким образом суд принял во внимание озабоченность бенефициарных владельцев по поводу неприкосновенности частной жизни.

В своем решении суд указал, что "доступ широкой общественности к информации о бенефициарной собственности представляет собой серьезное вмешательство в фундаментальные права на уважение частной жизни и защиту персональных данных".

По мнению Европейского суда, правила доступа, введенные в редакции Директивы 2018 года, в значительно большей степени ущемляют основные права физического лица, гарантированные статьями 7 и 8 Хартии прав человека ЕС, чем те, которые действовали ранее. При этом правовые гарантии Директивы, позволяющие субъектам данных эффективно защищать свои персональные данные от рисков злоупотреблений, недостаточны.

В результате этого нового решения национальные реестры прозрачности в Европейском Союзе должны оценить свои правила доступа. В свете решения Европейского суда доступ может стать гораздо более ограниченным.

Немецкий реестр прозрачности в настоящее время не удовлетворяет запросы представителей общественности на доступ до дальнейшего уведомления. С полудня 22 ноября 2022 года персональные данные о бенефициарных владельцах не передаются представителям общественности. Администратор немецкого реестра своевременно предоставит дополнительную информацию о дальнейших последствиях решения Европейского суда.





## Court of Justice of the European Union

*Judgment in Case C-453/21  
X-FAB Dresden GmbH & Co. KG v FC*

Суд Европейского Союза ("CJEU") 09.02.2023 вынес предварительное решение по делу C-453/21 X-FAB Dresden GmbH & Co. KG v FC по запросу Федерального суда по трудовым спорам Германии ("Суд по трудовым спорам") в отношении ст. 38(3) и 38(6) GDPR касательно увольнения сотрудника компании X-FAB с должности DPO.

CJEU постановил, что второе предложение ст.38(3) GDPR не препятствует принятию национального законодательства, предусматривающего, что контроллер или процессор может уволить внутреннего DPO только при наличии уважительной причины, даже если увольнение не связано с выполнением задач этого DPO, в той мере, в какой такое законодательство не подрывает достижение целей GDPR.

CJEU высказал мнение, что ст.38(6) GDPR должна быть истолкована как означающая, что "конфликт интересов" может существовать, когда на DPO возложены другие задачи или обязанности, в результате которых он будет определять цели и методы обработки персональных данных со стороны контроллера или его процессора. Существование конфликта интересов в таких случаях должен определять национальный суд в каждом конкретном случае, оценивая все соответствующие обстоятельства, включая организационную структуру контроллера или процессора, и, в свете всех применимых правил, любую политику контроллера или процессора.

## CJEU о необходимости получения согласий учителей на видеотрансляцию занятий



## Court of Justice of the European Union

*Judgment in Case C-34/21*

### *Principal Staff Committee for Teachers at the Hessian Ministry of Education v Hessian Ministry of Education*

В 2020 году Министерство высшего образования, исследований и искусств земли Гессен утвердило правила для школьного образования во время пандемии COVID-19, которые включали возможность для учеников посещать занятия в режиме видеоконференции при условии, что ученики или их родители предоставят свое согласие. Однако эти правила не включала положений, требующих согласия учителей, присутствующих на занятиях в режиме прямой трансляции. Министерство посчитало, что согласно ст.88(1) GDPR обработка персональных данных, связанная с прямой трансляцией занятий в режиме видеоконференции, подпадает под действие национального законодательства, поэтому она может осуществляться без получения согласия соответствующих учителей.

Эта позиция была оспорена Комитетом учителей в Административном суде Висбадена. Административный суд поддержал позицию Министерства, но обратился в Суд Европейского Союза ("CJEU") за предварительным решением в отношении того, совместимо ли данное национальное законодательство с условиями, изложенными в ст.88(2) GDPR.

CJEU 30.03.2023 постановил, что обработка персональных данных учителей во время прямой трансляции в режиме видеоконференции подпадает под материальную сферу действия GDPR. Применение национальных положений, обеспечивающих защиту прав и свобод работников в отношении обработки их персональных данных, должно быть отменено, если они не соответствуют условиям и ограничениям, установленным в статьях 88(1) и 88(2) GDPR, если только эти национальные положения не являются правовой основой согласно ст. 6(3) GDPR.

# CJEU об административных и гражданских средствах правовой защиты в соответствии с GDPR



## Court of Justice of the European Union

### Judgment in Case C-132/21

Физическое лицо воспользовалось своим правом доступа после посещения собрания, однако компания предоставила ему только выдержки из записи, в которых воспроизводились его собственные выступления, исключая выступления других участников, несмотря на то, что их выступления представляли собой ответы на заданные им вопросы.

После этого человек обратился в Национальный орган по защите данных и свободе информации Венгрии ("NAIH") с просьбой обязать соответствующую компанию выслать ему соответствующую запись. Поскольку NAIH отклонил запрос физического лица, физическое лицо подало административную апелляцию на решение NAIH в Высокий суд Будапешта. Физическое лицо также подало иск в гражданские суды Венгрии против решения данной компании отказать физическому лицу в доступе, который был основан на положениях GDPR. Высокий суд Будапешта поинтересовался у CJEU, связан ли он в контексте пересмотра законности решения NAIH окончательным решением гражданских судов по тем же фактам и тому же предполагаемому нарушению GDPR.

CJEU указал, что статьи 77(1), 78(1) и 79(1) GDPR предлагают различные средства правовой защиты лицам, при этом подразумевается, что каждое из этих средств правовой защиты должно быть способно быть использовано "без ущерба" для других. GDPR не предусматривает какой-либо приоритетной или исключительной компетенции или юрисдикции или какого-либо правила старшинства в отношении оценки, проводимой NAIH или судом, относительно того, имеет ли место нарушение соответствующих прав. Административные и гражданские средства правовой защиты, предусмотренные GDPR, могут применяться одновременно и независимо друг от друга.

## CJEU о праве на получение информации о раскрытии персональных данных



## Court of Justice of the European Union

### *Judgment in Case C-154/21*

CJEU опубликовал 12.03.2023 свое предварительное решение по делу о применимости ст.15(1) GDPR в споре между истцом и Österreichische Post AG после предварительного решения Верховного суда Австрии по тому же вопросу.

Спор возникли в контексте запроса заявителя в Österreichische Post о получении информации о том, какие персональные данные о нем Österreichische Post хранила или хранила в прошлом, и, если они были переданы третьим лицам, кто эти третьи лица. Österreichische Post ограничилась заявлением о том, что она использует данные в качестве издателя телефонных справочников и что она предлагает эти персональные данные деловым клиентам в маркетинговых целях, но не указала, кто является конкретными получателями этих данных.

Верховный суд Австрии постановил, что право доступа в соответствии со ст.15(1) GDPR распространяется не только на обрабатываемые персональные данные, но и на все данные, обработанные в прошлом. CJEU указал, что если данные были раскрыты получателям или продолжают раскрываться, ответственное лицо обязано проинформировать субъекта данных о личности получателя. Если невозможно идентифицировать получателей или если ответственное лицо не докажет, что запросы на доступ со стороны субъекта данных являются явно необоснованными или чрезмерными по смыслу ст.12(5) GDPR, ответственное лицо может только информировать субъекта данных о категориях соответствующих получателей.

В данном деле CJEU отметил, что Österreichische Post отклонила просьбу заявителя уведомить его о получателях, которым были раскрыты персональные данные, но Верховный суд Австрии должен рассмотреть вопрос о том, был ли запрос явно необоснованным или чрезмерным в соответствии со ст.12(5) GDPR.

# CJEU о возможности предъявления иска о возмещении ущерба при нарушении GDPR



## Court of Justice of the European Union

### Case C-300/21 UI v Österreichische Post AG

Суд ЕС вынес решение 04.05.2023 о том, что простого нарушения положений GDPR недостаточно для предъявления иска о возмещении ущерба. Необходимо, чтобы имело место фактическое нарушение GDPR. Субъект данных может требовать компенсации нематериального ущерба только тогда, когда он преодолевает определенный порог, который должен быть доказан. Однако в самой ст.82 GDPR не указано никаких критериев того, когда субъект данных может требовать возмещения нематериального ущерба. Считается, что простого расстройства из-за нарушения прав недостаточно. Однако возникает вопрос, является ли страх и постоянное подозрение в неправомерном использовании их персональных данных чем-то большим, чем простое расстройство. В деле с аналогичными обстоятельствами "простое раздражение", например, было расценено судом как недостаточное основание для требования возмещения убытков.

В другом деле с теми же обстоятельствами суд [принял решение](#), противоречащее позиции CJEU, и признал возможную кражу персональных данных нематериальным ущербом, который может быть взыскан с контроллера.

<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0300>

[https://gdprhub.eu/index.php?title=CJEU - Case C-300/21 - UI v %C3%96sterreichische Post AG](https://gdprhub.eu/index.php?title=CJEU_-_Case_C-300/21_-_UI_v_%C3%96sterreichische_Post_AG)

## Генеральный адвокат CJEU о нематериальном ущербе субъектам в случае утечки данных



27.04.2023 опубликовано заключение Джованни Питруцеллы – Генерального адвоката Суда Европейского Союза (‘CJEU’) по делу 340/21 VB v Natsionalna agentsia za prihodite. Заключение было вынесено в связи с обращением Верховного административного суда Болгарии к CJEU о вынесении предварительного решения относительно толкования GDPR в части условий присуждения компенсации за нематериальный ущерб лицу, чьи персональные данные, хранящиеся в государственном учреждении, были опубликованы в интернете в результате хакерской атаки.

Само по себе возникновение нарушения персональных данных не означает, что технические и организационные меры, принятые контролером данных, не были надлежащими для обеспечения защиты данных. Напротив, национальные суды должны определить, были ли принятые меры надлежащими на практике, проведя конкретный анализ содержания этих мер и способа их применения, а также их практического эффекта. Бремя доказывания того, что принятые меры были надлежащими, лежит на контролере данных, который может быть освобожден от ответственности в том случае, если он сможет продемонстрировать, что он никоим образом не несет ответственности за событие, приведшее к ущербу.

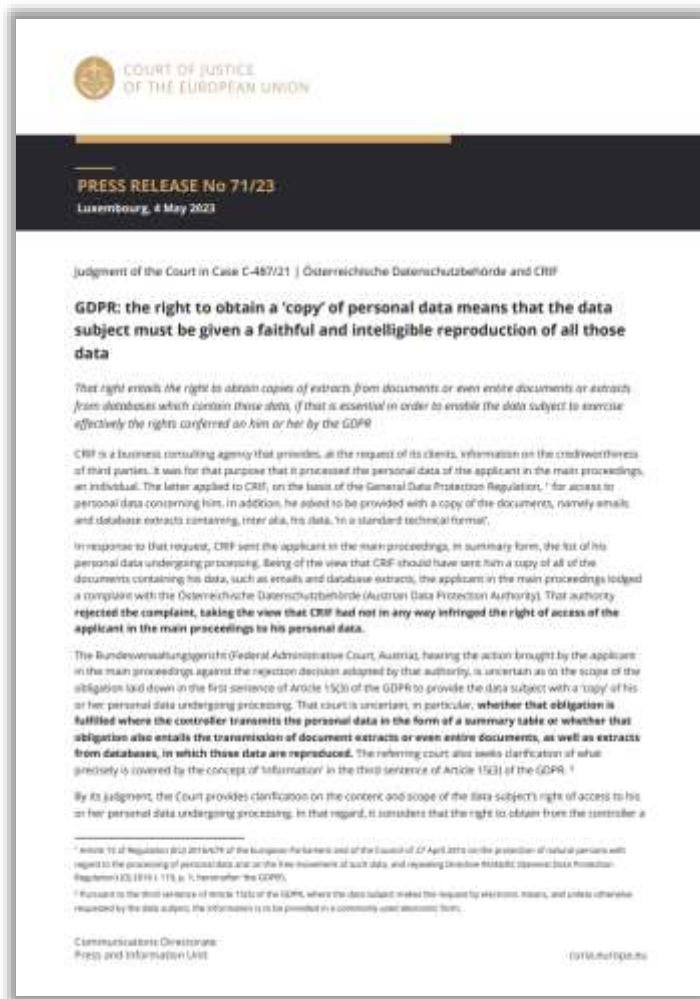
Страх перед возможным неправомерным использованием их персональных данных в будущем может представлять собой нематериальный ущерб, дающий право на компенсацию субъекту данных, при условии, что субъект данных докажет, что он понес реальный и определенный эмоциональный ущерб, что в каждом конкретном случае должен проверить компетентный национальный суд.

## Генеральный адвокат CJEU о понятии (совместного) контроллера, обработки и строгой ответственности



Предыстория дела такова: приложение для отслеживания COVID было первоначально разработано компанией ITSS по инициативе NVSC (государственный орган). В уведомлениях о конфиденциальности упоминалась NVSC. Однако в итоге NVSC так и не приобрела права на приложение у компании-разработчика. В результате возник вопрос, кто должен считаться контролером. АГ заявил, что контролером является только тот, кто фактически определяет средства обработки и кто фактически дал согласие на выпуск мобильного приложения для общественности. АГ также заявил, что отсутствие официального соглашения не препятствует квалификации отношений как совместного контроля. Совместный контроль возникает в ситуации, когда обработка была бы невозможна без участия обеих сторон, поскольку обе стороны оказывают ощутимое влияние на определение целей и средств такой обработки, а не просто координируют свои действия. АГ также заявил, что запуск тестовой фазы приложения считается "обработкой" (duh). Наконец, что, вероятно, наиболее важно, АГ заявил, что, по его мнению, ответственность за нарушение GDPR может наступить только в том случае, если оно произошло "намеренно или по халатности".

## CJEU: сводная таблица не является достаточным ответом на запрос о доступе к данным



Решение, похоже, полностью соответствует мнению AG, высказанному ранее: сводной таблицы обработанных данных недостаточно, необходимо предоставить выдержки из документов или даже целые документы. Это может подорвать некоторые бизнес-модели, в которых внутренняя конфиденциальность данных является конкурентным преимуществом.



# CJEU о возможности предъявления иска о возмещении ущерба при нарушении GDPR



## Court of Justice of the European Union

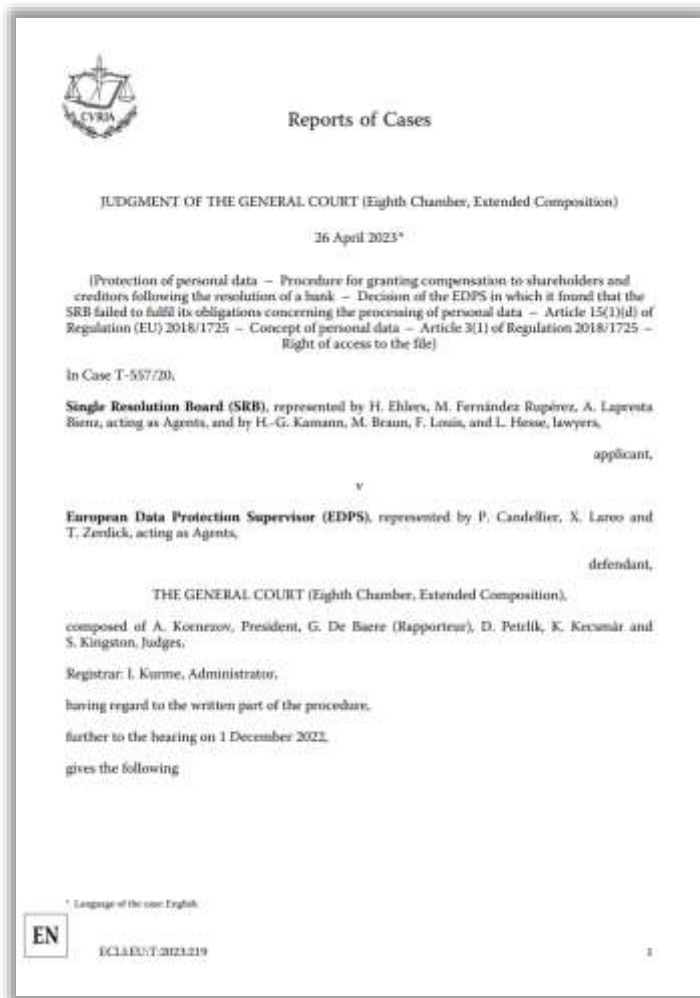
*Case C-579/21 - Pankki S*

Суд ЕС постановил, что сотрудники контролера не могут рассматриваться как "получатели" в значении Статьи 15(1)(с) GDPR, когда они обрабатывают персональные данные под руководством этого контролера в соответствии с его инструкциями.

Однако, несмотря на то, что сотрудники не считаются получателями, CJEU отметил, что информация о лицах, которые обращались к персональным данным субъекта данных, содержащаяся в журнале регистрации, может представлять собой персональные данные субъекта данных согласно статье 4(1) GDPR, что позволяет субъекту данных проверить законность обработки его данных и, в частности, убедиться в том, что операции по обработке действительно осуществлялись под руководством контролера и в соответствии с его инструкциями.

CJEU, кроме того, напомнил, что право доступа не должно негативно сказываться на правах и свободах других лиц. Даже если раскрытие личности сотрудников контролера субъекту данных может быть необходимо ему для обеспечения законности обработки, оно, тем не менее, может нарушить права и свободы этих сотрудников. В случае конфликта между, с одной стороны, i.) реализацией права доступа и, с другой стороны, ii.) правами или свободами других лиц, необходимо будет найти баланс между этими правами и свободами.

## CJEU: псевдонимизированные данные, отправленные получателю - не персональные, если получатель не имеет возможности установить субъектов

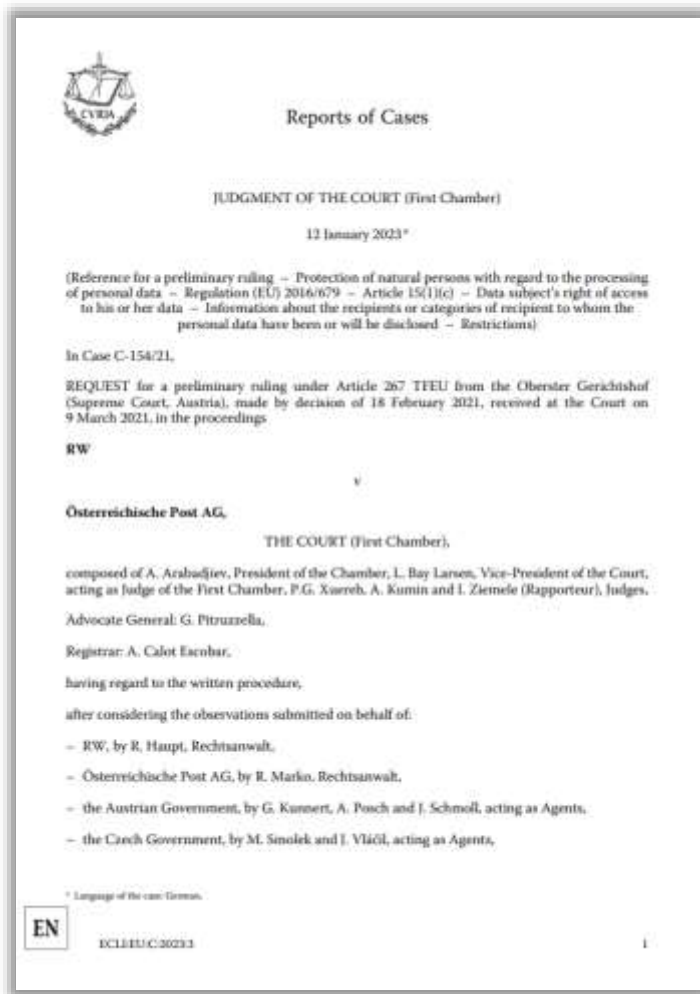


Нормативное руководство ЕС и прецедентное право CJEU (например, Beyer) всегда устанавливали невозможно высокий стандарт для анонимизации. Однако решение Генерального суда ЕС по делу T-557/20, SRB v EDPS, дает проблеск надежды на то, что анонимизация может быть легче достижима.

Предыстория: SRB обратилась к частным лицам с просьбой представить свои комментарии через электронную форму. Имена были заменены случайным 33-значным буквенно-цифровым кодом. SRB предоставила данные с ключевым кодом третьей стороне. Третья сторона не имела средств для повторной идентификации субъектов данных. EDPS решил, что данные, переданные получателю, являются псевдонимизированными только потому, что SRB располагает дополнительной информацией для декодирования данных. Европейский суд отменил это решение. Основные выводы:

- необходимо учитывать точку зрения получателей данных при рассмотрении вопроса о том, являются ли данные персональными;
- псевдонимизированные данные, переданные получателю, будут анонимными данными, если у получателя нет средств для повторной идентификации субъекта данных;
- тот факт, что отправитель данных имеет средства для повторной идентификации субъектов данных, не имеет значения и не означает, что переданные данные автоматически также являются персональными данными для получателя.

## 1075 CJEU о детализации описания получателей данных в RoPA



По мнению CJEU, после передачи персональных данных третьим лицам необходимо отслеживать их реальную принадлежность. Простого упоминания "специалиста по маркетингу", "поставщика услуг по расчету заработной платы" или "кадрового агентства" в RoPA под названием "получатели" может быть уже недостаточно.

В RoPA необходимо отслеживать фактическое название/идентификацию компаний или лиц, с которыми персональные данные были переданы или передаются. Таким образом, если субъект данных (например, клиенты, сотрудники и т.д.) спросит вас: "Кому вы передали мои персональные данные и как с ними связаться?", вы сможете предоставить ему обоснованный ответ, а не список общих категорий получателей.

Неполные или неконкретные ответы на запрос субъекта данных в отношении состава получателей персональных данных могут привести к нарушению ст. 5(1)(a), 12 и/или 13(1)(e) GDPR.

## 1076 CJEU о законности резервного копирования базы с персональными данными

Суд Европейского Союза (CJEU) 20.10.2022 вынес решение по делу C-77/21 Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, касающееся запроса на вынесение предварительного решения, поданного судом Будапешта (Budapest-Capital). Решение касается спора между одним из ведущих интернет-провайдеров и вещательных компаний Венгрии и Национальным управлением по защите данных и свободе информации ("NAIH") в связи с нарушением персональных данных, содержащихся в базе данных, принадлежащей первому.

CJEU пришел к выводу, что:

- ст.5(1)(b) GDPR должна быть истолкована как означающая, что принцип ограничения цели не препятствует регистрации и хранению контролером данных в базе данных, созданной для проведения тестов и исправления ошибок, персональных данных, ранее собранных и сохраненных в другой базе данных, если такая дальнейшая обработка совместима с конкретными целями, для которых персональные данные были первоначально собраны; это обстоятельство должно определяться в свете критериев, упомянутых в статье 6(4) GDPR;
- ст.5(1)(e) GDPR должна быть истолкована как означающая, что принцип ограничения хранения не позволяет контролеру данных хранить персональные данные, ранее собранные для других целей, в базе данных, созданной для проведения тестов и исправления ошибок, в течение периода времени, превышающего тот, который необходим для осуществления указанной деятельности.

## CJEU: Facebook должен получать согласие жителей ЕС на сбор их данных для рекламы



Европейский суд 04.07.2023 постановил, что Facebook на территории Евросоюза не должен улучшать свои сервисы на основе пользовательских данных и показывать пользователям персонализированную рекламу без согласия пользователей. Иначе говоря, правовая основа в виде исполнения договора и/или законного интереса не подходит для Facebook – "учитывая масштаб этой обработки и ее значительное влияние на пользователя, а также тот факт, что пользователь не может разумно ожидать, что эти данные будут обрабатываться".

Использование данных со сторонних сайтов в рекламных целях противоречит GDPR и является злоупотреблением доминирующим положением со стороны компании Meta на рынке социальных платформ. Сам факт посещения пользователем сайтов или приложений, которые могут раскрывать личную информацию, еще не означает, что он согласен делиться этими данными.

Федеральное антимонопольное ведомство Германии в 2019 году запретило Meta использовать информацию со сторонних сайтов в рекламных целях, поскольку это, по мнению его экспертов, противоречило GDPR. Однако компания посчитала, что ведомство не имело полномочий принимать подобные решения и обратилась в суд высшей инстанции. Европейский суд постановил, что антимонопольные органы стран ЕС могут самостоятельно проверять действия компаний на предмет их соответствия правилам GDPR в том случае, если предполагается, что речь может идти о злоупотреблениях.

## Генеральный адвокат CJEU: доступ к IP-адресу разрешены для расследования нарушений авторских прав в Интернете

◇ 28.09.2023 Суд Европейского Союза (CJEU) опубликовал пресс-релиз, содержащий краткое изложение заключения генерального адвоката (AG) Мацея Шпунара по делу C-470/21 La Quadrature du Net и другие. CJEU пояснил, что заключение было вынесено в контексте возобновления производства по данному делу и что AG впервые высказал свое мнение в октябре 2022 года.

◇ Запрос на вынесение предварительного решения поступил от Государственного совета Франции после судебного разбирательства, возбужденного четырьмя ассоциациями по защите прав и свобод в Интернете. В ходе судебного разбирательства оспаривался принятый в 2010 г. декрет, позволяющий Высшему органу Франции по распространению произведений и защите прав в Интернете (Hadopi) требовать от операторов электронных коммуникаций предоставления гражданских идентификационных данных пользователя, которому присвоен IP-адрес, используемый для совершения нарушения авторских прав.

◇ AG посчитал, что законодательство ЕС не препятствует требованию к провайдерам услуг электронных коммуникаций хранить IP-адреса и соответствующие гражданские идентификационные данные, а также не препятствует административному органу, ответственному за защиту авторских прав, получать доступ к таким адресам и данным. В этой связи AG посчитал, что IP-адрес, гражданская идентификация лица, имеющего право на доступ в Интернет, и информация, касающаяся соответствующих действий, не позволяют сделать точные выводы о частной жизни лица, предположительно нарушившего авторские права. По мнению AG, все, что было выявлено, - это просмотр контента в определенное время, что само по себе не позволяет составить подробный профиль лица, просматривавшего контент.

◇ AG высказал мнение, что сохранение и доступ к гражданским идентификационным данным, связанным с используемым IP-адресом, должны быть разрешены в случаях, когда эти данные являются единственным средством расследования, позволяющим идентифицировать нарушителей авторских прав, совершенных исключительно в Интернете. Механизм поэтапного реагирования, принятый Hadopi в соответствии с оспариваемым постановлением, совместим с требованиями законодательства ЕС в области защиты персональных данных.

## **CJEU: пациент имеет право на бесплатное получение первой копии медицинской карты независимо от причин запроса**

Суд Европейского Союза (CJEU) 26.10.2023 объявил о своем решении по делу FT v DW (C-307/22), вынесенном в тот же день по запросу Федерального суда Германии о вынесении предварительного решения по делу, возбужденному пациентом, который хотел бесплатно получить копию своей медицинской карты у стоматолога, чтобы привлечь его к ответственности за ошибки, якобы допущенные при оказании стоматологической помощи. Однако стоматолог потребовал от пациента оплатить расходы, связанные с предоставлением копии медицинской карты, как это предусмотрено немецким законодательством.


CJEU напомнил, что GDPR закрепляет право пациента на получение первой копии своей медицинской карты без каких-либо затрат, пояснив, что контролер данных может взимать плату только в том случае, если пациент уже получил первую копию данных бесплатно.

CJEU пришел к выводу, что национальные правила не могут заставить пациента нести расходы на получение первой копии его медицинской карты. В рассматриваемом случае CJEU постановил, что стоматолог, как контролер данных, обязан предоставить пациенту первую копию его данных бесплатно, а пациент не обязан объяснять причины своего запроса.

Наконец, CJEU разъяснил, что пациент имеет право получить полную копию документов, включенных в его медицинскую карту, если это необходимо для понимания персональных данных, содержащихся в этих документах. По мнению CJEU, это право распространяется на данные, содержащиеся в медицинской документации, в которых содержится информация о диагнозах, результатах обследований, оценках лечащих врачей, а также о любом проведенном лечении или изобретениях.

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-10/cp230161en.pdf>

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=279125&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=3509117>



Reports of Cases

OPINION OF ADVOCATE GENERAL  
CAMPOS SÁNCHEZ-BORDONA  
delivered on 4 May 2023<sup>1</sup>

Case C-319/22

**Gesamtverband Autoteile-Handel e.V.**  
v  
**Scania CV AB**

(Request for a preliminary ruling from the Landgericht Köln (Regional Court, Cologne, Germany))

(Reference for a preliminary ruling – Market for motor vehicle repair and maintenance information services – Regulation (EU) 2018/858 – Independent operators – Information easily accessible in a machine-readable format that is capable of being electronically processed – Vehicle identification number (VIN) – Protection of personal data – Regulation (EU) 2016/679 – Conditions for lawful processing of personal data – Article 6(1)(c))

1. The EU legislature aims to ensure competition in the motor vehicle repair and maintenance sector, within the internal market, in such a way that vehicle manufacturers do not monopolise (by themselves or through their authorised dealers and workshops) the supply of those services.
2. For that purpose, Regulation (EU) 2018/858<sup>2</sup> requires automotive manufacturers to provide 'independent operators' with unrestricted, standardised and non-discriminatory access to information on certain vehicle systems, equipment and tools and their repair and maintenance.
3. The application of Regulation 2018/858 (or some of the regulations which it amends) has led to disputes between vehicle manufacturers, on the one hand, and independent operators, on the other. Certain requests for a preliminary ruling come from proceedings in which an entity<sup>3</sup> whose members are responsible for 80% of the turnover of the motor vehicle parts aftermarket in Germany has been involved.<sup>4</sup>

<sup>1</sup> Original language: Spanish.

<sup>2</sup> Regulation of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ 2018 L 151, p. 1).

<sup>3</sup> Gesamtverband Autoteile-Handel e.V. (Gesamtverband A.-H.).

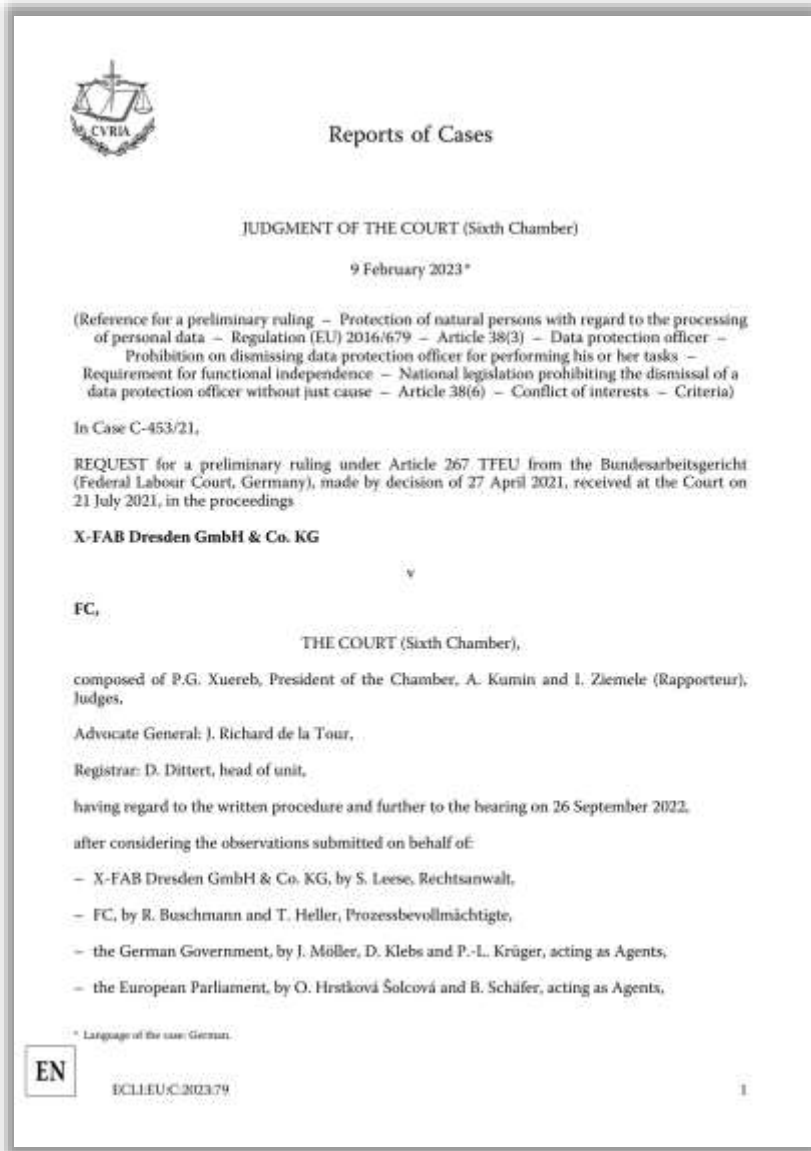
<sup>4</sup> Judgments of 19 September 2019, Gesamtverband Autoteile-Handel (C-527/18, EU:C:2019:762), and of 27 October 2022, ADPA and Gesamtverband Autoteile-Handel (C-390/21, EU:C:2022:837).

**EN** ECLI:EU:C:2023:385 1

Европейский суд (CJEU) 09.11.2023 постановил по делу C-319/22 Gesamtverband Autoteile-Handel, что идентификационные номера транспортных средств (VIN), сами по себе, не являются персональными данными. Однако они становятся персональными данными по смыслу ст. 4(1) GDPR в той мере, в какой лицо, имеющее доступ к VIN, может располагать средствами, позволяющими ему использовать VIN для идентификации владельца транспортного средства, к которому он относится. Вопрос о том, имеет ли это место в каждом конкретном случае, должен решать суд. При принятии решения суд сослался также на параграфы 42 и 43 дела Breyer (C 582/14, EU:C:2016:779).



## CJEU: совмещение позиции председателя рабочего совета и DPO ведет к конфликту интересов



Европейский суд (CJEU) 09.02.2023 постановил по делу C-453/21 X-Fab Dresden GmbH & Co. KG, что каждое государство-член может устанавливать более конкретные правила, касающиеся увольнения DPO, при условии, что эти правила совместимы с законодательством ЕС и GDPR. CJEU также постановил, что "конфликт интересов", согласно статье 38(3) GDPR, может иметь место, когда на DPO возложены другие задачи или обязанности, в результате чего он/она определяет цели и методы обработки персональных данных от имени обработчика/контролера.

Ранее субъект данных был сотрудником контроллера, компании X-FAB (производство полупроводников), и занимал в компании две должности: он был председателем рабочего совета и DPO в X-Fab и других компаниях той же группы предприятий. Однако 01.12.2017 субъект данных был отстранен от исполнения своих обязанностей в качестве DPO по просьбе DPA земли Тюринген (TLfDI) (Германия). В качестве меры предосторожности другие предприятия также приняли решение о его увольнении на основании второго предложения ст.38(3) GDPR, которое стало применимым за прошедший период.

<https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-453/21>

[https://gdprhub.eu/index.php?title=CJEU - C-453/21 - X-Fab Dresden GmbH %26 Co. KG](https://gdprhub.eu/index.php?title=CJEU_-_C-453/21_-_X-Fab_Dresden_GmbH_%26_Co._KG)

## CJEU: "скоринг" рассматривается как "автоматизированное индивидуальное решение" в соответствии со ст.22 GDPR

**COURT OF JUSTICE  
OF THE EUROPEAN UNION**

**PRESS RELEASE No 186/23**  
Luxembourg, 7 December 2023

Judgments of the Court of Justice in Case C-634/21 | SCHUFA Holding (Scoring) and in Joined Cases C-26/22 and C-64/22 | SCHUFA Holding (Discharge from remaining debts)

**The General Data Protection Regulation (GDPR) opposes two data processing practices by credit information agencies**

While 'scoring' is permitted only under certain conditions, the prolonged retention of information relating to the granting of a discharge from remaining debts is contrary to the GDPR.

A number of members of the public are challenging the refusal of the competent data protection commissioner to take action against certain activities of SCHUFA, a private company providing credit information for clients including banks, before the Administrative Court of Wiesbaden (Germany). Specifically, they are opposed to 'scoring' and to the storage of information relating to the granting of a discharge from remaining debts taken from public registers.

'Scoring' is a mathematical statistical method used to predict the probability of future behaviour, such as the repayment of a loan. Information relating to the granting of a discharge from remaining debts is kept in the German public insolvency register for six months, while a code of conduct for German credit information agencies stipulates a retention period of three years for their own databases. The administrative court asks the Court of Justice to clarify the scope of personal data protection as provided for by the General Data Protection Regulation (GDPR).

As regards 'scoring', the Court holds that it **must be regarded as an 'automated individual decision' prohibited in principle by the GDPR, in so far as SCHUFA's clients, such as banks, attribute to it a determining role in the granting of credit.** According to the Administrative Court of Wiesbaden, this is the case. It is for that court to assess whether the German Federal Law on data protection contains a valid exception to that prohibition in accordance with the GDPR. If this is the case, it will still have to check whether the general conditions laid down by the GDPR for data processing have been met.

As regards information relating to the granting of a **discharge from remaining debts, the Court considers that it is contrary to the GDPR for private agencies to keep such data for longer than the public insolvency register.** The discharge from remaining debts is intended to allow the data subject to re-enter economic life and is therefore of existential importance to that person. That information is still used as a negative factor when assessing the solvency of the data subject. In this case, the German legislature has provided for data to be stored for **six months**. It therefore considers that, at the end of the six months, the rights and interests of the data subject take precedence over those of the public to have access to that information.

**In so far as the retention of data is unlawful, as is the case beyond six months, the data subject has the right to have the data deleted and the agency is obliged to delete the data as soon as possible.**

As regards the **parallel storage** of such information by SCHUFA **for those six months**, it is for the Administrative Court to **weigh up the interests involved** in order to assess its lawfulness. Should it conclude that parallel storage for six months is lawful, the data subject will still have the right to object to the processing of his or her data and the right to have the data erased, unless SCHUFA can demonstrate the existence of overriding legitimate grounds.

Communications Directorate  
Press and Information Unit

curia.europa.eu

Европейский суд (CJEU) 07.12.2023 постановил по делам C-634/21 OQ v Land Hessen, C-26/22 и C-64/22 UF/AB v Land Hessen в связи с запросами Административного суда Висбадена о вынесении предварительного решения в отношении практики SCHUFA Holding (SCHUFA), частного агентства, предоставляющего кредитную информацию.

CJEU высказал мнение, что "скоринг" должен рассматриваться как "автоматизированное индивидуальное решение", и в той мере, в какой клиенты SCHUFA (например, банки) приписывают ему определяющую роль в выдаче кредита, он будет запрещен в принципе ст.22 GDPR. CJEU также отметил, что административный суд обязан оценить, содержит ли Федеральный закон о защите данных от 30 июня 2017 года (имплементирующий GDPR) действительное исключение из этого запрета, отметив, однако, что в этом случае административный суд все равно должен проверить, были ли соблюдены общие условия, установленные GDPR для обработки данных.



Европейский суд (CJEU) 05.12.2023 в постановлениях по делам C-579/21 Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija и C-807/21 Deutsche Wohnen SE v Staatsanwaltschaft Berlin высказал мнение, что национальный орган по надзору за защитой данных (DPA) не может налагать штраф на контролера данных за нарушение GDPR, если только это нарушение не было совершено противоправно, то есть намеренно или по халатности. Противоправное нарушение может иметь место, если контролер не мог не знать о нарушающем характере своего поведения, независимо от того, было ли ему известно о нарушении или нет.

В случае, когда контролером является юридическое лицо, не обязательно, чтобы нарушение было совершено его органом управления, равно как и не обязательно, чтобы этот орган знал о таком нарушении. Контроллер также может быть оштрафован в отношении операций, выполненных процессором, в той степени, в которой контроллер может быть признан ответственным за такие операции.

В тех случаях, когда адресатом штрафа является предприятие или его часть, DPA должен взять за основу концепцию "предприятия" в соответствии с антимонопольным законодательством ЕС. Соответственно, для расчета штрафа CJEU разъяснил, что DPA должно учитывать общий мировой оборот всей группы за предыдущий рабочий год.

## CJEU: возможное неправомерное использование персональных данных может представлять собой нематериальный ущерб



Европейский суд (CJEU) 14.12.2023 постановил по делу C-340/21 VB v Natsionalna agentsia za prihodite, о компенсации морального ущерба, понесенного физическим лицом в результате предполагаемого невыполнения контролером, государственным учреждением, своих юридических обязательств в отношении обработки персональных данных.

Ст.82(1) GDPR должна толковаться в том смысле, что страх перед потенциальным неправомерным использованием персональных данных субъекта данных третьими лицами после нарушения GDPR сам по себе может представлять собой моральный ущерб в смысле ст.82(1) GDPR.

Контролеры обязаны возместить ущерб, возникший в результате несанкционированного раскрытия персональных данных или несанкционированного доступа к ним третьих лиц. Однако контролеры могут быть освобождены от этого обязательства, если докажут, что факт, вызвавший ущерб, никак не связан с контролером.

Кроме того, несанкционированное раскрытие персональных данных или несанкционированный доступ к ним третьих лиц в значении ст.4(10) GDPR сами по себе не являются достаточными для того, чтобы считать, что технические и организационные меры, предпринятые данным контролером, не были надлежащими в значении статей 24 и 32 GDPR.

Контролер несет бремя доказывания целесообразности мер безопасности, которые он реализовал в соответствии со ст.82 GDPR. Оценка целесообразности мер безопасности, реализованных контролером данных, должна быть сделана конкретным образом.

# CJEU: статья 82(1) GDPR должна выполнять компенсационную, а не карательную функцию



Recueil de la jurisprudence

ARRÊT DE LA COUR (troisième chambre)

21 décembre 2023\*

« Renvoi préjudiciel – Protection des personnes physiques à l’égard du traitement des données à caractère personnel – Règlement (UE) 2016/679 – Article 6, paragraphe 1 – Conditions de licéité du traitement – Article 9, paragraphes 1 à 3 – Traitement portant sur des catégories particulières de données – Données concernant la santé – Appréciation de la capacité de travail d’un employé – Service médical en matière d’assurance maladie traitant des données relatives à la santé de ses propres employés – Admissibilité et conditions d’un tel traitement – Article 82, paragraphe 1 – Droit à réparation et responsabilité – Réparation d’un préjudice moral – Fonction compensatoire – Incidence de la faute commise par le responsable du traitement »

Dans l’affaire C-667/21,

ayant pour objet une demande de décision préjudicielle au titre de l’article 267 TFUE, introduite par le Bundesarbeitsgericht (Cour fédérale du travail, Allemagne), par décision du 26 août 2021, parvenue à la Cour le 8 novembre 2021, dans la procédure

**ZQ**

contre

**Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts,**

LA COUR (troisième chambre),

composée de M<sup>me</sup> K. Jürimäe, présidente de chambre, MM. N. Piçarra, M. Safjan, N. Jääskinen (rapporteur) et M. Gavalec, juges,

avocat général : M. M. Campos Sánchez-Bordona,

greffier : M. A. Calot Escobar,

vu la procédure écrite,

considérant les observations présentées :

– pour ZQ, par M<sup>e</sup> E. Daun, Rechtsanwalt,

\* Langue de procédure : l’allemand.

FR

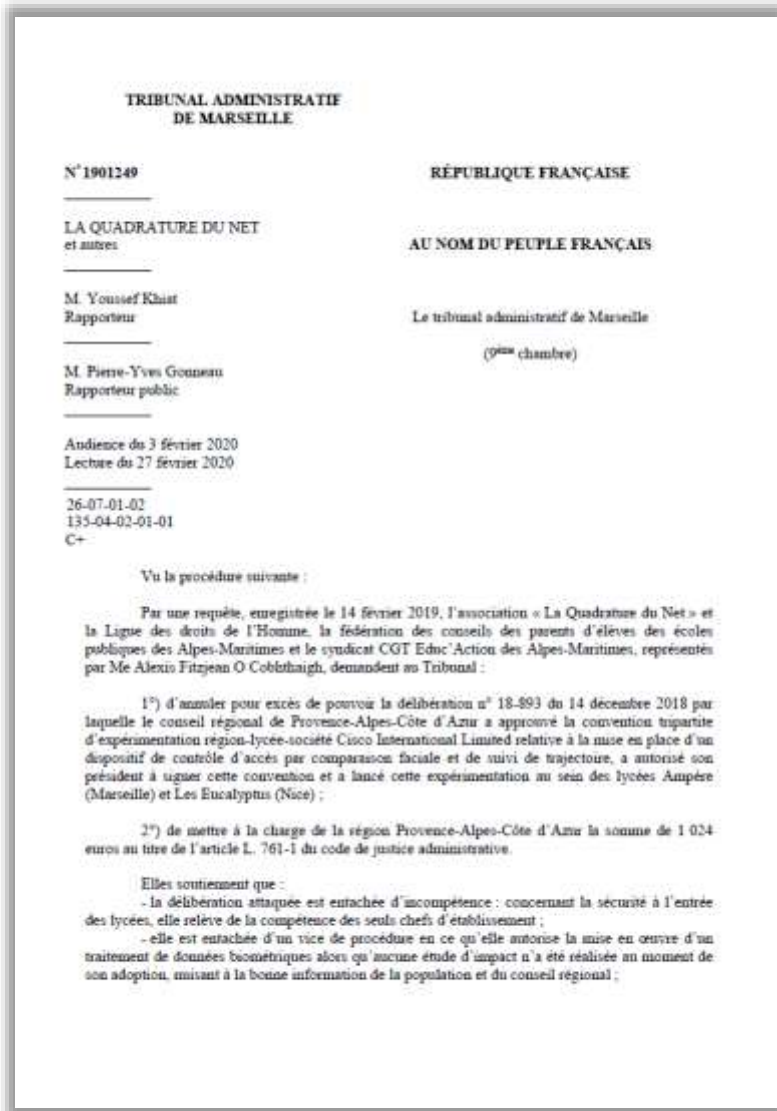
ECJ:EU:C:2023:1022

1

Европейский суд (CJEU) 21.12.2023 вынес постановление по делу C-667/21 ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts, касающегося MDK Nordrhein, медицинской службы больничной кассы Германии, которая проводит медицинские экспертизы, связанные с нетрудоспособностью лиц, застрахованных в кассе обязательного медицинского страхования.

Одним из выводов суда является то, что ст.82(1) GDPR должна толковаться в том смысле, что она выполняет компенсационную функцию, поскольку финансовая компенсация, основанная на этом положении, должна позволять полностью компенсировать ущерб субъекту данных, фактически понесенный в результате нарушения GDPR, а не сдерживающую или карательную функцию.

# Административный суд Марселя признал незаконным использование системы распознавания лиц в школах



## Tribunal Administratif de Marseille

Административный суд Марселя 03.02.2020 признал незаконным использование системы распознавания лиц на входах в школах Ницце и Марселе. Указанные системы были внедрены на основании решения администрации региона «Прованс-Альпы-Лазурный Берег» (Provence-Alpes-Côte d'Azur), принятого 12.2019.

Суд постановил, что только сами школы имеют полномочия на принятие решений о внедрении систем распознавания лиц. Кроме того, суд установил, что обработка биометрических персональных данных осуществлялась на основании согласий учеников и их законных представителей, которые были даны в ситуации «дисбаланса» положения контролера и субъекта данных, а также отсутствия у последних реальной свободы выбора.

Наконец, Административный суд согласился с позицией CNIL о том, что распознавание лиц является непропорциональной мерой контроля для пропуска учащихся в школу. Более того, альтернативные меры гораздо менее ущемляют права людей.

## 1087 Отмена штрафа в €575,000 на компанию VoetbalTV



23.11.2020 нидерландский суд отменил решение голландского управления по защите данных (Autoriteit Persoonsgegevens) о наложении штрафа в €575,000 на компанию VoetbalTV, которая ведет видеозаписи матчей любительских футбольных клубов (в т.ч. несовершеннолетних футболистов) и является социальной платформой, где более 500,000 пользователей смотрели, анализировали матчи и делились записями с другими. Причиной штрафа является наличие у платформы только коммерческого интереса в создании и трансляции видеозаписей матчей, но отсутствие у неё законного интереса для этого.

По мнению VoetbalTV, не смотря на наличие у них коммерческого интереса, видеозаписи также имеют журналистский и информационный характер и делают спорт доступным для широкой аудитории. Суд не согласен с компанией в том, что видеозаписи матчей имеют журналистскую (новостную) ценность. Однако суд посчитал, что наличие коммерческого интереса не исключает возможность наличия законного интереса. По мнению суда, Autoriteit Persoonsgegevens должно расследовать ситуацию с учетом всех обстоятельств деятельности VoetbalTV.

# Решение Royal Court of Justice в части территориальной применимости GDPR



Neutral Citation Number: [2021] EWHC 56 (QB)

**IN THE HIGH COURT OF JUSTICE**  
**QUEEN'S BENCH DIVISION**  
**MEDIA AND COMMUNICATIONS LIST**

Case No: QB-2020-002450

Royal Courts of Justice  
Strand, London, WC2A 2LL

Date: 15/01/2021

Before:

**MR JUSTICE JAY**

Between :

WALTER TZVI SORIANO

Claimant

- and -

(1) FORENSIC NEWS LLC

(2) SCOTT STEDMAN

(3) ERIC LEVAI

(4) JESS COLEMAN

(5) ROBERT DENAULT

(6) RICHARD SILVERSTEIN

Defendants

Greg Callus and Ben Hamer (instructed by Rechtschaffen Law Offices) for the Claimant  
Jonathan Price (instructed by Gibson, Dunn and Crutcher UK LLP) for the First to Fifth  
Defendants

The Sixth Defendant was neither present nor represented

Hearing dates: 14<sup>th</sup> and 15<sup>th</sup> December 2020

## Approved Judgment

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

Covid-19 Protocol: This judgment was handed down by the judge remotely by circulation to the parties' representatives by email and release to Bailii. The date and time for hand-down is deemed to be Friday 15<sup>th</sup> January 2021 at 10.00am.

MR JUSTICE JAY

MR JUSTICE JAY  
Approved Judgment

Soriano v Forensic News LLC [2021] EWHC 56 (QB)

- basis, and which in any event can be cancelled at any time, amounts to arrangements which are sufficient in nature, number and type to fulfil the language and spirit of article 3.1 and amount to being "stable". To the extent that it improves the Claimant's case slightly, the 7<sup>th</sup> August tweet post-dated all of the publications sued on.
65. For the purposes of article 3.1, it is unnecessary to consider whether the processing at issue was "in the context of" the activities of a controller or processor established in the EU. The Claimant's case falls at the first hurdle.
66. As for article 3.2(a), there is nothing to suggest that the First Defendant is targeting the United Kingdom as regards the goods and services it offers. That this country is a potential shipping destination for merchandise which in the event does not appear to have been purchased by anyone here (save possibly for one baseball cap) does not in my opinion fulfil sub-para (a) as explained in the EDPB Guidelines. No more than a cursory examination of their listed indicia serves to demonstrate how far short the Claimant comes in meeting this sub-para.
67. I also accept Mr Price's submission that the clause "are related to" is narrower and stricter than the phrase "in the context of". As the EDPB has observed, a data controller may be subject to the GDPR in respect of some of its processing activities and not others. The Claimant must demonstrate that the activity in sub-para (a) (sc. the offering of goods and services) is related to the First Defendant's core activity, namely its journalism; and in my judgment it is not. It is not enough for the Claimant to show that the First Defendant may have carried out some processing which is related to the offering of goods and services in this jurisdiction (I have concluded that it has not), or that such processing may have been in the context of what I am characterising the First Defendant's core activity.
68. As for article 3.2(b), I can accept that the Claimant has an arguable case that the First Defendant's use of cookies etc. is for the purpose of behavioural profiling or monitoring, but that is purely in the context of directing advertisement content. There is no evidence that the use of cookies has anything to do with the "monitoring" which forms the basis of the Claimant's real complaint: the Defendant's journalistic activities have been advanced not through any deployment of these cookies but by using the internet as an investigative tool. In my judgment, that is not the sort of "monitoring" that article 3.2(b) has in mind; or, put another way, the monitoring that does properly fall within this provision – the behavioural profiling that informs advertising choices – is not related to the processing that the Claimant complains about (assuming that carrying out research online about the Claimant amounts to monitoring at all).
69. I therefore conclude that the Claimant has no arguable case under the GDPR. I should add for completeness that had I reached a different conclusion on the merits I would have found in favour of the Claimant on *forum conveniens*. Mr Callus rightly points out that the claim under the GDPR would have to be brought in the courts of a Member State of the EU. There is nothing to suggest that England and Wales would have been other than the most natural and appropriate forum for trial, and no evidence that such a claim could be brought in the US.

*The Second Issue: the Malicious Falsehood Claim*



JDSUPRA®

August 31, 2018

## German Art Copyright Act Applies Even With GDPR In Effect

KING & SPALDING

On June 18, 2018, the Cologne Court of Appeal decided that provisions of the German Act on the Protection of Copyright in Works of Art and Photographs (“KUG”) regarding the publication of photos for journalistic reporting will prevail over conflicting provisions of the General Data Protection Regulation (“GDPR”) (Docket number 15 W 27/18).

The applicant had filed a cease and desist claim to prevent a television program from being released. He briefly was depicted as a security guard in a report on the eviction of a building. In the first instance, the Regional Court of Cologne held that the respondent’s freedom of the press and freedom of expression prevailed over the applicant’s right to his own image. The judges applied Section 23(1) No. 1 of the KUG, which allows images of historical importance to be published without a person’s consent. The term “historical importance” covers not only events of historical-political significance, but all current and historical events of general social interest.

**Oberlandesgericht Köln**

*Case 15 W 27/18*

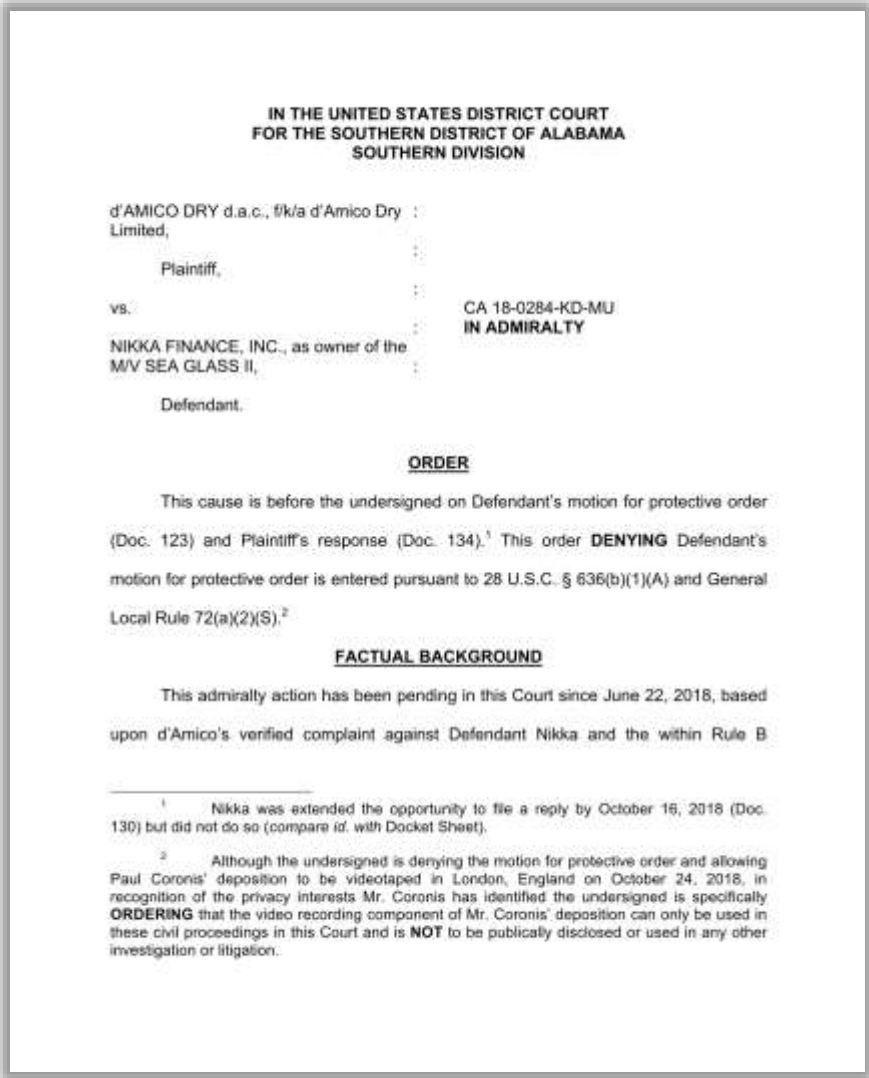
*Decision on 18 June 2018*

Верховный окружной суд в Кёльне постановил, что положения Закона Германии о защите авторских прав на произведения искусства и фотографии («KUG»), касающиеся публикации фотографий для журналистских репортажей, будут иметь преимущественную силу в отношении положений GDPR.

Суд отказал в удовлетворении иска лица, которое попало на видеозапись репортажа. В первой инстанции суд Кельна постановил, что свобода прессы и свобода выражения мнения ответчика имеют преимущество над правом истца на использование собственного видеоизображения. Судом был применен Раздел 23(1) №1 KUG, который позволяет публиковать изображения исторического значения без согласия запечатлённого на них лица, так как термин «историческое значение» охватывает не только события историко-политического значения, но и все текущие и исторические события, представляющие общественный интерес.

Magistrate Judge P. Bradley Murray

Американский суд постановил, что права гражданина ЕС на неприкосновенность частной жизни и соблюдение положений GDPR не имеют преимуществ над правом американского истца на предъявление доказательств, в том числе показаний ответчика, снятых на видеокамеру.





The image is a screenshot of a BBC News article. At the top, there is a navigation bar with the BBC logo, a 'Sign in' button, and several category tabs: News, Sport, Reel, Worklife, Travel, and Future. Below this is a prominent red banner with the word 'NEWS' in white. Underneath the banner is another navigation bar with tabs for Home, Video, World, UK, Business, Tech, Science, Stories, and Entertainment & Arts. The main headline of the article is 'Google wins landmark right to be forgotten case'. Below the headline, it says 'By Leo Kelion, Technology desk editor' and '24 September 2019'. The article text begins with a bolded summary: 'The EU's top court has ruled that Google does not have to apply the right to be forgotten globally.' This is followed by a paragraph explaining that it means the firm only needs to remove links from its search results in Europe - and not elsewhere - after receiving an appropriate request. The next paragraph states that the ruling stems from a dispute between Google and a French privacy regulator. The following paragraph mentions that in 2015, CNIL ordered the firm to globally remove search result listings to pages containing damaging or false information about a person. The next paragraph notes that the following year, Google introduced a geoblocking feature that prevents European users from being able to see delisted links. The final paragraph states that Google resisted censoring search results for people in other parts of the world and that the firm challenged a 100,000 (\$109,901; £88,376) euro fine that CNIL had tried to impose.

## Court of Justice of the European Union

Европейский суд справедливости (CJEU) поддержал позицию Google в давнем споре с французским регулятором CNIL о локализации права на забвение резидентов ЕС и неправомерности фактического введения режима «глобальной цензуры» путем расширительной интерпретации территориальной сферы применения GDPR. Кроме того, был отменен ранее наложенный на Google штраф в €100,000.


BUSINESS INSIDER

TECH FINANCE POLITICS STRATEGY LIFE ALL

SI PRIME INTELLIGENCE

### Prince Harry won a legal battle with the paparazzi using Europe's GDPR privacy law — and it gives the royals a powerful new weapon against the media

Kieran Conrath May 22, 2019, 11:17 AM



Prince Harry gives an interview on camera after Meghan Markle gave birth to the couple's first child, a boy they named Archie. Getty Images

Prince Harry this week notched another victory in the royal family's long-running battle with paparazzi photographers, securing a "substantial payout" from an agency which used a helicopter to take pictures inside a house he was renting.

Potentially even more interesting than that is the way in which he won his battle — basing a legal case partly on a sweeping new European data law that is less than a year old.

According to a statement delivered to London's High Court on Thursday, in which the paparazzi agency Splash News apologized to Harry, also known as the Duke of Sussex (emphasis ours):

"This matter concerns a claim for misuse of private information, breaches of The Duke's right to privacy under Article 8 ECHR and breaches of the **General Data Protection Regulation ("GDPR")** and Data Protection Act 2018 ("DPA")."

Royals and celebrities arguing that media coverage invades their privacy is relatively well-trodden ground. Prince William and Kate Middleton famously won a payout from the French edition of Closer magazine on privacy grounds after it published topless photographs of Middleton while she was on holiday in Provence.

Принц Гарри одержал победу в судебном споре с фотографами папарацци из агентства Splash News, которое использовало вертолет для фотографирования используемого принцем дома и его окрестностей. В Высоком суде Лондона агентство извинилось перед принцем и согласилось выплатить ему компенсацию за нарушение ст.5 GDPR и британского Закона о защите данных 2018 (DPA) в связи с неправомерной обработкой его персональных данных и нарушением права на неприкосновенность частной жизни.

Согласно мнению Тимоти Пинто, старшего юриста юридической фирмы Taylor Wessing, использование положений GDPR является потенциально привлекательной альтернативой искам о нарушении неприкосновенности частной жизни: «Чтобы преуспеть в иске о диффамации, заявитель должен установить, по крайней мере, что: (i) заявление, на в отношении которого подан иск, дискредитирует истца; и (ii) был нанесен ущерб репутации истца. Напротив, истец, опирающийся на закон о защите данных, не должен доказывать ни одну из этих вещей».

COVINGTON

# Inside Privacy

*Updates on developments in data privacy and cybersecurity*

FROM COVINGTON & BURLING LLP

[HOME](#) > [ADVERTISING & MARKETING](#) > [MOBILE](#) > GERMAN COURT DECIDES THAT GDPR CONSENT CAN BE TIED TO RECEIVING ADVERTISING

## German court decides that GDPR consent can be tied to receiving advertising

*By Kristof Van Quathem and Anna Oberschelp de Meneses on September 4, 2019*

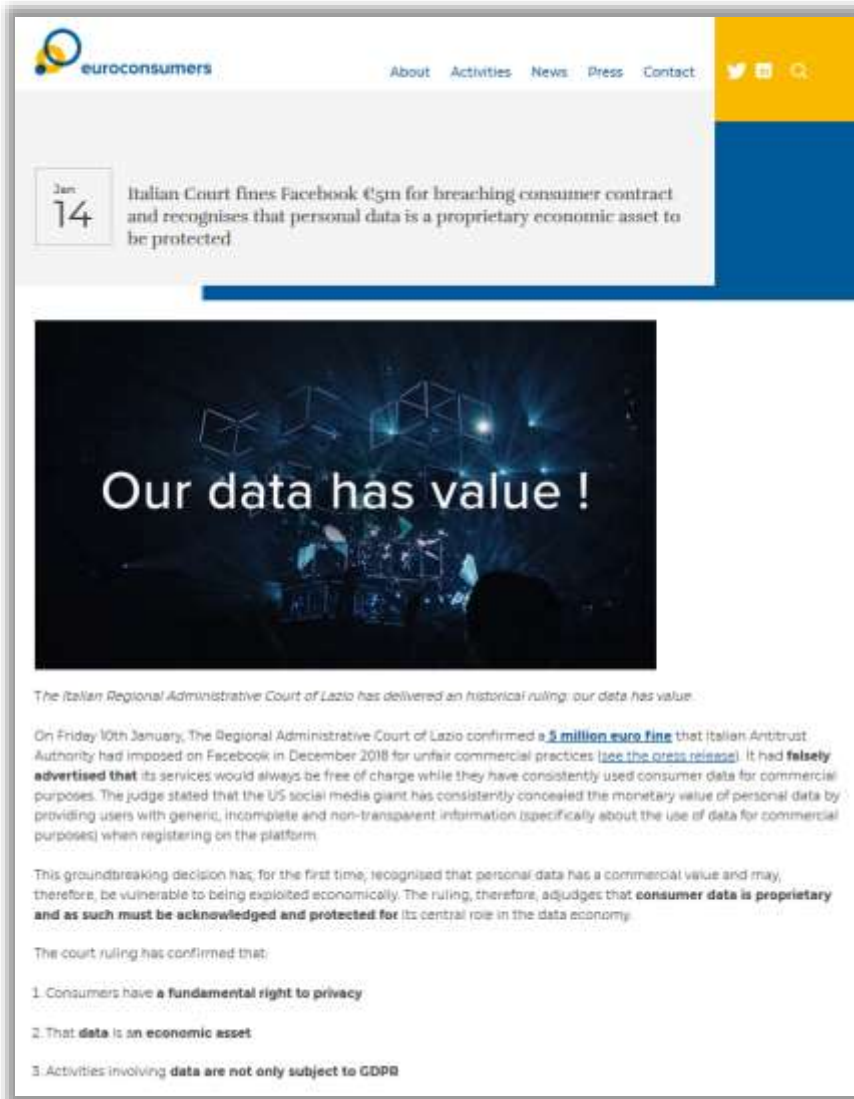
POSTED IN [EU DATA PROTECTION](#), [EUROPEAN UNION](#), [MOBILE](#)

On June 27, 2019, the High Court of Frankfurt **decided** that a consent for data processing tied to a consent for receiving advertising can be considered as freely given under the GDPR.

The case concerned an electricity company that relied on consent obtained by another company to advertise its products and services to the claimant. The claimant's consent had been obtained in connection with his participation in a sweepstakes contest. In order for the claimant to participate in the contest, he had to consent to receive advertising from partners of the sweepstakes company, including the electricity company. The claimant was provided with a list of the eight companies with whom his data would be shared for advertising purposes.

27.06.2019 Высокий суд Франкфурта (High Court of Frankfurt) постановил, что согласие на обработку данных, связанное с согласием на получение рекламы, может считаться свободно предоставленным в рамках ст.7(4) GDPR. По мнению суда, «свободно даваемое» согласие - это согласие, которое дается без «принуждения» или «давления». Суд постановил, что привлечение клиента обещанием скидки или участия в розыгрыше лотереи в обмен на согласие на обработку его данных для рекламы не составляет такого принуждения или давления. По мнению суда, «потребитель может и должен сам решать, стоит ли участие в лотереях его или ее данных».

## 1094 Персональные данные имеют экономическое значение



The screenshot shows the website 'euroconsumers' with a navigation menu (About, Activities, News, Press, Contact) and social media icons. A date widget shows 'Jan 14'. The main headline reads: 'Italian Court fines Facebook €5m for breaching consumer contract and recognises that personal data is a proprietary economic asset to be protected'. Below the headline is a large image with the text 'Our data has value!' and a background of a person's silhouette looking at a digital data visualization. The article text below the image states: 'The Italian Regional Administrative Court of Lazio has delivered an historical ruling: our data has value. On Friday 10th January, The Regional Administrative Court of Lazio confirmed a 5 million euro fine that Italian Antitrust Authority had imposed on Facebook in December 2018 for unfair commercial practices (see the press release). It had falsely advertised that its services would always be free of charge while they have consistently used consumer data for commercial purposes. The judge stated that the US social media giant has consistently concealed the monetary value of personal data by providing users with generic, incomplete and non-transparent information (specifically about the use of data for commercial purposes) when registering on the platform. This groundbreaking decision has, for the first time, recognised that personal data has a commercial value and may, therefore, be vulnerable to being exploited economically. The ruling, therefore, adjudges that consumer data is proprietary and as such must be acknowledged and protected for its central role in the data economy. The court ruling has confirmed that: 1. Consumers have a fundamental right to privacy 2. That data is an economic asset 3. Activities involving data are not only subject to GDPR'.

10.01.2020 Областной административный суд Лацио (Il Tribunale Amministrativo Regionale per il Lazio) отклонил апелляцию Facebook Ireland Ltd. в отношении штрафа (€5,000,000 в отношении Facebook Ireland Ltd. и на аналогичную сумму для ее материнской компании Facebook Inc.), назначенного в декабре 2018 года Управлением по защите конкуренции и рынка в Италии (L'Autorità Garante della Concorrenza e del Mercato) за нарушение ст. 21 и 22 Codice del Consumo (Кодекса потребителей Италии). Суд подтвердил, что законы о защите потребителей также применяются к обработке персональных данных из-за их экономической ценности.

## 1095 Снижение штрафа с €9,550,000 до всего лишь €900,000



11 ноября 2020 года Боннский окружной суд (Landgericht) снизил размер штрафа более чем на 90% (с €9,550,000 до всего лишь €900,000), который был ранее наложен на поставщика телекоммуникационных услуг 1&1 Telecom GmbH Федеральным комиссаром Германии по защите данных и свободе информации (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit - BfDI) в связи с предполагаемым нарушением безопасности обработки персональных данных в соответствии со ст.32(1) GDPR. Таким образом, исходя из соответствующего оборота группы контролёра в €3,660,000,000, штраф составил только 0,025%.

Хотя суд Бонна согласился с позицией BfDI о том, что на самом деле имело место (предсказуемое и виновное) нарушение ст.32(1) GDPR со стороны 1 & 1 Telecom GmbH, суд также установил, что Руководящие принципы наложения административных штрафов, принятые 16.10.2019 18 немецкими DPA, не соответствуют требованиям ст.83 GDPR. Суд подверг критике Руководящие принципы за слишком большое внимание к обороту контролёра, заключив, что первая и основная функция оборота - определение потенциального максимального штрафа за нарушение GDPR, а не определение конкретной суммы штрафа. В частности, оборот не входит в число критериев, установленных ст.83(2) GDPR для определения размера административного штрафа. При этом суд заключил, что в качестве первого шага DPA необходимо было определить размер штрафа независимо от оборота только на основании ст.82(2) GDPR, и только если такой штраф будет слишком низким (и, следовательно, неэффективным и не сдерживающим) или слишком высоким (и, следовательно, несоразмерным) по отношению к сумме оборота, штраф может быть увеличен или уменьшен.

## 1096 Отмена компенсации ущерба субъекту персональных данных

The screenshot shows the Raad van State website interface. At the top left is the logo 'Raad van State'. To its right are links for 'hoog contrast' and 'lees voor'. Below the logo is a navigation bar with 'Actueel', 'Adviezen', and 'Uitspraken'. A breadcrumb trail reads 'U bent hier: Home > Uitspraken > Uitspraak 201902699/1/A2'. The main heading is 'Uitspraak 201902699/1/A2'. Below this, there is a table with the following information:

ECLI:	ECLI:NL:RVS:2020:900
Datum uitspraak:	1 april 2020
Inhoudsindicatie:	Bij besluit van 16 augustus 2016 heeft het college van burgemeester en wethouders van Borsele naar aanleiding van het verzoek van [appellant] op grond van de Wet bescherming persoonsgegevens (hierna: Wbp) medegedeeld dat de NAW (naam, adres en woonplaats)- gegevens van [appellant] in het digitale postregistratiesysteem van de gemeente Borsele zijn verwerkt om zijn verzoeken op grond van de Wet openbaarheid bestuur (Wob) te registreren en om brieven aan te kunnen maken, verzenden en registreren. Voorts heeft het college [appellant] bericht geen aanleiding te zien om een overzicht te geven van teksten die op het forum van de Vereniging Nederlandse Gemeenten (VNG) zijn geplaatst, omdat het forum een besloten discussieplatform voor ambtenaren betreft en het niet gaat om verwerking van persoonsgegevens.

At the bottom of the page, there are two tags: 'eerste aanleg - meervoudig' and 'persoonsgegevens'.

Консультативная коллегия Государственного совета Нидерландов (Raad van State) 01.04.2020 года решила отменить решение нижестоящей инстанции, вынесенное на основании ст.82 GDPR, о присуждении субъекту персональных данных компенсации размере €500 вследствие вреда, возникшего из-за неправомерной передачи персональных данных субъекта между несколькими муниципалитетами. Государственный совет постановил, что формальное нарушение фундаментальных прав субъекта персональных данных не означает автоматического нанесения субъекту ущерба. Кроме того, Государственный совет указал, что в соответствии со статьей 6:106(1)(b) Гражданского кодекса Нидерландов бремя доказывания факта ущерба лежит на истце (субъекте), и что в рассматриваемом деле истец не смог доказать наличие этого факта.

Кроме того, Государственный совет заявил, что в GDPR не установлен механизм определения размера ущерба, и что Европейский суд еще не вынес решения по вопросу о расчете компенсации, связанной с нарушениями конфиденциальности. Наконец, Государственный совет установил, что противоправная передача между муниципалитетами сведений об имени и месте жительства субъекта не квалифицируется как серьезное правонарушение, так как не было представлено доказательств дальнейшего противоправного использования персональных данных.



## Решение Федерального конституционного суда Германии по ст.82(1) GDPR о возмещении ущерба субъекту



14.01.2021 немецкий суд отказал в удовлетворении иска субъекта о возмещении ему ущерба в соответствии со ст.82(1) GDPR, связанного с направлением маркетингового электронного письма на рабочий адрес электронной почты истца без его согласия. Суд отметил, что дело касалось всего лишь одного электронного письма, которое не было получено в критический момент времени для субъекта, было четко обозначено как реклама и не требовало длительного рассмотрения. Таким образом, порог существенности ущерба от правонарушения для предоставления компенсации не был достигнут.

Это решение соответствовало прецедентному праву Федерального конституционного суда, применимому к нематериальному ущербу в соответствии с гражданским законодательством Германии: если истцы запрашивают такой нематериальный ущерб, они должны доказать, что действие или бездействие привело к серьезному нарушению их личных прав.

**Следует отметить, что в п.п. 85, 146 преамбулы и ст.82 GDPR нет четких указаний на критерий существенности ущерба в отношении предоставления компенсации субъектам.**

## Субъекту данных необходимо доказывать факт нанесения ущерба в случаях нарушения GDPR



### Employment Germany

#### Go west – damages for transferring personal employee data to the US?

By Dr. Kai Bosenstedt LL.M. / 20 April 2021 / Compliance, Data Protection, Model Clauses, Transfer of Employee Data to the US

As part of a judgement dated 25 February 2021 (docket number: 17 Sa 37/20), the Baden-Wuerttemberg Labour Court of Appeals (the second out of three levels of the German labor court system) has clarified the requirements for an entitlement to immaterial damages in cases of a violation of the General Data Protection Regulation (GDPR). Over recent years, German employees across the country have identified and abused privacy-related GDPR instruments such as data subject access requests to try and gain leverage in settlement negotiations. More recently, claims for damages have also become en vogue in this respect. In this recent ruling, the Baden-Wuerttemberg Labour Court of Appeals has confirmed that, unlike DSARs, such damage claims are not low-hanging fruits for employees. In particular, the reasoning of the ruling will be helpful for companies to argue that the threshold of the burden of proof for damages is quite high. While the decision also provides interesting annotations on the requirements of standard contractual clauses within the meaning of the GDPR, the court did not need to address the scope of a possible entitlement to immaterial damages. As this question is repeatedly raised in courts, it becomes more and more likely that the European Court of Justice will have to rule on this issue in the near future.

**Facts:**

The subject of the dispute was the employee's alleged entitlement to immaterial damages in connection with the transfer of his personal data to the employer's parent company in the US. The employer prepared to introduce a cloud-based HR information management system ("HR System"). In order to test the HR System, during April and May of 2017 the employer transferred the employee's personal data to a workshare page of its parent company without the employee's consent. The employer and the responsible works council agreed a works agreement on the use of the HR System and established categories of data to be used temporarily for this purpose. The personal data of the employees which were transferred were (at least in part) not covered by the works agreement. On 24 May 2018, one day before the effective date of GDPR, the employer and its US-based parent company concluded a comprehensive agreement on the processing of data and its protection. The employee argued that the transfer of his personal data constituted a violation of GDPR since there was no legal basis for the transfer. He further argued that this unlawful state had existed for almost two years and that it was possible that the data had been transferred to authorities within the US. The employee further claimed that he should be awarded immaterial damages for the violation of his privacy rights.

Апелляционный суд по трудовым спорам земли Баден-Вюртемберг 25.02.2021 разъяснил требования для права на получение нематериального ущерба в случаях нарушения GDPR.

По мнению суда, бремя доказывания того, что нарушение GDPR привело к ущербу, ложится на истца, то есть на субъекта данных, и этот порог бремени доказывания ущерба довольно высок.

Простая возможность неправомерного использования или передачи данных сама по себе недостаточна, чтобы показать, что истец понес убытки.

## 1099 Юрист подал в суд на юриста из-за нарушений GDPR на веб-сайте

LG Würzburg, Beschluss v. 13.09.2018 – 11 O 1741/18 UWG

**Titel:**  
Wettbewerbsrechtlicher Unterlassungsanspruch wegen der Nichteinhaltung der DSGVO

**Normenketten:**  
UWG § 3 a, § 4 Nr. 11, § 8 Abs. 3, § 12 Abs. 2, § 14 Abs. 2  
ZPO § 32, § 92 Abs. 2 Ziff. 1, § 880 Abs. 1, § 937 Abs. 2

**Leitsatz:**  
Ein Rechtsanwalt hat ggÜ einer Wettbewerberin einen Anspruch auf Unterlassung des Betriebes einer für deren berufliche Tätigkeit als Rechtsanwältin unverschlüsselte Website, die keine DSGVO-konforme Datenschutzerklärung enthält. (redaktioneller Leitsatz)

**Schlagwort:**  
Rechtsbruch

**Fundstellen:**  
NWSt 2018, 3143  
WfRP 2018, 1400  
K & R 2018, 736  
MDR 2018, 1362  
AnwB 2018, 660  
BRAB-Mit 2018, 315  
BeckRS 2018, 22735  
LSK 2018, 22735  
ZD 2018, 38  
GRUR-RS 2018, 22735

**Tenor**

I. Der Antraggegnerin wird untersagt, für ihre berufliche Tätigkeit als Rechtsanwältin die unverschlüsselte Homepage www... ohne Datenschutzerklärung nach der Datenschutz-Grundverordnung der EU (DSGVO 2016/679) vom 27.04.2016 in deren Geltungsbereich zu betreiben.

II. Der Antraggegnerin wird für jeden Fall der Zuwiderhandlung die Verhängung eines Ordnungsgeldes von bis zu 250.000,00 €, ersatzweise Ordnungshaft bis zu 2 Jahren, sowie die Verhängung einer Ordnungshaft von bis zu 6 Monaten angedroht.

III. Im übrigen wird der Antrag zurückgewiesen.

IV. Die Antraggegnerin hat die Kosten des Verfahrens zu tragen.

V. Der Streitwert wird auf 2.000,00 € festgesetzt.

**Gründe**

**1**  
Die Zuständigkeit des Gerichts ergibt sich hier aus § 14 Abs. 2 UWG (Begehungsort, liegender Gerichtsstand bezüglich des Internets) und nicht aus § 32 ZPO wie von Antragstellerseite angegeben.

**2**  
Dem Antragsteller steht ein Verfügungsanspruch auf Unterlassung zu, das der Antragsteller glaubhaft gemacht hat, dass die Antraggegnerin bezüglich ihrer Homepage gegen die Datenschutzgrundverordnung (DSGVO), die spätestens seit 25.05.2018 umzusetzen ist verstößt. Die im Impressum der Antraggegnerin enthaltene 7-zellige Datenschutzerklärung genügt der neuen DSGVO nicht. Es fehlen Angaben zum/zur Verantwortlichen, zur Erhebung und Speicherung personenbezogener Daten sowie Art und Zweck deren

У некоего немецкого юриста был свой сайт. На этом сайте не было уведомления об обработке персональных данных (cookie-баннер). В добавок к этому сайт не был защищен SSL шифрованием.

На это обратил внимание другой юрист и подал на своего коллегу по цеху в суд. В итоге суд не обязал владельца сайта платить штрафы, но запретил ответчику пользоваться своим сайтом до тех пор, пока он не получит SSL сертификат и не опубликует уведомление об обработке персональных данных согласно требованиям ст. 5(1)(a), 13 и 32 GDPR.

## Словения: право на забвение не позволяет удалить персональные данные из церковного реестра крещений

Приход Римско-католической церкви (далее - Приход), будучи контролером данных, рассматривал заявление физического лица на право на забвение (удаление данных). Субъект попросил удалить его персональные данные из реестра крещения (далее - Реестр), потому что он больше не был членом церкви. По его мнению, собранные данные больше не нужны по отношению к целям, для которых они были собраны. Он не давал согласия на крещение и обработку персональных данных. Субъект также утверждал, что персональные данные (имя и фамилия субъекта крещения, дата рождения, дата крещения, имена родителей и крестных родителей, а также место жительства), внесенные в Реестр, свидетельствуют о религиозных убеждениях и ущемляют его религиозную свободу.

**Приход утверждал**, что правовой основой для обработки данных в Реестре является, в основном, Закон о защите документов и архивов и архивных учреждениях (далее - Закон), который классифицирует Реестр как архивный материал выдающегося национального значения, поэтому не разрешается удалять какие-либо содержащиеся в нем данные. Приход также сделал дополнительную запись в Реестре о том, что данное лицо больше не является членом церкви.

**Комиссар по информации Республики Словения** (далее - Регулятор) оценил, необходима ли обработка для целей архивирования в общественных интересах в соответствии со ст.89(1) GDPR, и может ли удаление сделать невозможным или серьезно помешать достижению целей этой обработки (ст.17(3)(d) GDPR). Регулятор подчеркнул, что сам вышеуказанный Закон предусматривает, что церковный документальный материал имеет характеристики архивного материала. Он также подчиняется принципам постоянства и целостности и предусматривает меры, которые могут рассматриваться как соответствующие меры безопасности в соответствии со ст. 89(1) GDPR. Регулятор решил, что Реестр является архивным документом в соответствии с национальным законом и что физическое лицо не может требовать права на удаление, когда обработка необходима для целей архивирования в общественных интересах. Удаление данных серьезно затруднит достижение этих целей.

Решение Регулятора было обжаловано в суде, но **Административный суд** в октября 2021 года подтвердил решение Регулятора и добавил, что обработка не связана с религиозными элементами только потому, что Приход хранит его данные в Реестре. Запись в Реестре ясно демонстрирует, что лицо больше не является членом церкви, что также свидетельствует о его праве не принадлежать к определенной религии.

## Франция: право на забвение не позволяет удалить персональные данные из церковного реестра крещений

15.02.2020 года субъект данных подал жалобу в надзорный орган Франции ("CNIL") в связи с отказом Епархиальной ассоциации Анже удовлетворить его запрос на доступ к персональным данным о нем, содержащимся в реестре крещений епархии Анже, а также на осуществление его права на удаление и возражение против обработки его персональных данных.

Отметив, что запрос на доступ был удовлетворен контролером, CNIL посчитал, что (i) субъект данных не может ссылаться ни на одно из оснований для удаления, упомянутых в ст.17(1) GDPR, и (ii) вставка на полях регистра заявления о том, что субъект данных не признает ценность своего крещения, может рассматриваться как удовлетворение его права на возражение в соответствии со ст.21(1) GDPR. Поэтому в письме от 02.12.2021 CNIL проинформировал субъекта данных о своем решении закрыть жалобу.

Субъект данных обжаловал это решение, попросив Высший административный суд Франции ("Conseil d'Etat") отменить его. Суд отметил, что реестры крещений, которые ведет католическая церковь, предназначены для регистрации каждого события. Эти персональные данные были доступны только заинтересованным лицам, а сами реестры хранились в закрытом месте до передачи в исторический архив епархии в течение 120 лет. Высший административный суд Франции 02.02.2024 постановил, что право на удаление данных из регистра крещений невозможно из-за того, что церковь имела более весомое законное основание для обработки данных.

## Google проиграл во французском суде дело о 100 млн евро штрафа за принуждение пользователей разрешить cookies

Silicon.co.uk

### French Court Upholds 100m Euro Fine On Google Over Cookies

Tom Jowitt, January 31, 2022, 4:21 pm



Google has been told by French court it has to pay a \$112m fine, over forcing use of advertising tracking cookies on people's devices

Alphabet's Google division has suffered a setback in French courts, after it rejected an attempt to annual a stiff regulatory fine.

Французский суд 28.01.2021 утвердил штраф в размере 100 миллионов евро, выписанный Google за нарушения, связанные с политикой использования файлов cookie. Штраф, наложенный французским органом по защите данных CNIL, соразмерен правонарушению, говорится в заявлении суда.

Он был выписан в декабре 2020 года, и на тот момент был крупнейшим штрафом, наложенным французским надзорным органом. CNIL тогда обнаружил, что французские сайты Google не запрашивали предварительного согласия посетителей до того, как рекламные файлы cookie были сохранены на компьютерах, и заявил, что Google не предоставил четкой информации о том, как он намеревался их использовать.

## Верховный суд Австрии подтвердил законность портала поиска и рейтинга врачей

### Ausgewählte Entscheidungen der Gerichte

#### OGH-Urteil vom 29.08.2022, 6 Ob 198/21t

In dieser Entscheidung hat das Höchstgericht der Revision einer Betroffenen (Ärztin) und der Ärztekammer für Wien nicht Folge gegeben. Die Sache betrifft die Datenverarbeitung durch die Betreiberin (Ges.m.b.H.) eines Such- und Bewertungsportals für Ärzte (siehe auch DSB, 23.01.2019, DSB-D123.342/0001-DSB/2019, RIS).

Der OGH hat eine umfassende Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO vorgenommen. Die Verantwortliche nimmt sowohl eigene berechnete Interessen als auch solche der Nutzer ihres Portals wahr. Sie kann sich dabei sowohl auf Art. 11 EU-Grundrechtecharta – GRC (Informationsfreiheit) als auch auf Art. 16 GRC (Unternehmerfreiheit) stützen. Die Verarbeitung ist notwendig, da es für den angestrebten Zweck auf eine möglichst vollständige Erfassung aller niedergelassenen Ärzte ankommt. Berechnete Interessen der (Erst-) Klägerin und Betroffenen können sich auf Art. 7 und 8 GRC (Privatleben, Datenschutz) sowie ebenfalls Art. 16 GRC stützen. Diese überwiegen jedoch nicht. Die Verarbeitung betrifft nur die Sozial-sphäre, nicht den höchstpersönlichen Lebensbereich der Ärztin. Ausschlaggebend war wohl das laut OGH „ganz erhebliche Interesse, das die Öffentlichkeit an den im Portal angebotenen Informationen und Möglichkeiten hat“, in Verbindung mit der Tatsache, dass die Verantwortliche ein Melde- und Beschwerdesystem zum Schutz gegen Missbrauch des Bewertungssystems eingerichtet hat.

Верховный суд Австрии 29.08.2022 вынес решение № 6 Ob 198/21t, в котором не поддержал апелляцию субъекта данных, врача, и Венской медицинской ассоциации в деле об обработке их персональных данных оператором портала поиска и рейтинга врачей. В частности, суд установил правомерность обработки персональных данных в соответствии со ст.6(1)(f) GDPR (законный интерес контролера или третьих лиц).

Суд постановил, что контролер данных, оператор портала поиска и рейтинга врачей, защищал свои законные интересы, а также интересы пользователей своего портала, опираясь при этом на статьи 11 и 16 Европейской хартии основных прав ЕС, поскольку обработка данных была необходима для достижения намеченной цели - иметь полную информацию обо всех врачах, занимающихся частной практикой.

Суд отметил значительный интерес, который общественность проявляет к информации и возможностям, предлагаемым на рейтинговом портале, в связи с тем, что оператор портала создал систему проверки сведений для защиты врачей от злоупотребления системой рейтинга.

## Федеральный административный суд Австрии подтвердил особый характер данных, используемых для рекламы

### BVwG-Erkenntnis vom 11.7.2022, GZ: W176 2246272/1/4E

Mit diesem Erkenntnis bestätigte das BVwG die Rechtsansicht der Datenschutzbehörde, wonach es sich bei statistisch ermittelten Wahrscheinlichkeitswerten, die der mitbeteiligten Partei seitens der Verantwortlichen zugeschrieben worden sind, um Daten besonderer Kategorie iSd Art. 9 DSGVO handelt.

Die Datenschutzbehörde hatte sich in zahlreichen Fällen mit der Frage auseinanderzusetzen, ob die Verarbeitung der aus der Sozialforschung stammenden „Sinus-Geo Milieus“ durch die datenschutzrechtlich Verantwortliche unter den Anwendungsbereich des Art. 9 DSGVO fällt.

Die gegenständlichen Daten stellen statistisch errechnete Wahrscheinlichkeitswerte dar, die der Betroffenen zugeschrieben wurden, um dieser gezielt Werbung übermitteln zu können.

Folgende Begriffe samt Übereinstimmung ausdrückender Prozentpunkte wurden dieser zugeordnet: *Konservative, Traditionelle, Etablierte, Performer, Postmaterielle, Digitale Individualisten, Bürgerliche Mitte, Adaptiv Pragmatische, Konsumorientierte Basis, Hedonisten.*

Das Bundesverwaltungsgericht bestätigte, dass aus diesen Zuschreibungen vermeintliche weltanschauliche Überzeugungen der Betroffenen hervorgehen und es sich bei den Sinus Geo-Milieus sohin um Daten besonderer Kategorie iSd Art. 9 DSGVO handelt.

Das BVwG führte außerdem aus, dass es unerheblich sei, dass die Verantwortliche die Daten von einer Dritten bezogen hatte, da sie diese in weiterer Folge in ihrer eigenen Datenbank verarbeitete.

Festzuhalten ist, dass bereits mit Erkenntnis vom 30.05.2022, Zl. W108 2246273-1/10E, erstmalig die Rechtsansicht der DSB bestätigt wurde.

Федеральный административный суд Австрии опубликовал 11.07.2022 свое решение по делу № W176 2246272/1/4E, в котором подтвердил правовое заключение австрийского органа по защите данных ("DSB"), согласно которому статистически определенные значения вероятности, присвоенные (назначенные) контролером лицу, являются данными специальной категории в значении ст.9 GDPR.

Данные, о которых идет речь, представляют собой предположение об идеологических/политических убеждениях лица для того, чтобы иметь возможность отправлять ему целевую (таргетированную) рекламу. Кроме того, суд отметил, что не имеет значения тот факт, что контролер получил данные от третьей стороны, поскольку впоследствии он обработал их в собственной базе данных.



## Окружной суд Мюнхена признал cookie-баннер BurdaForward нарушающим требования TTDSG

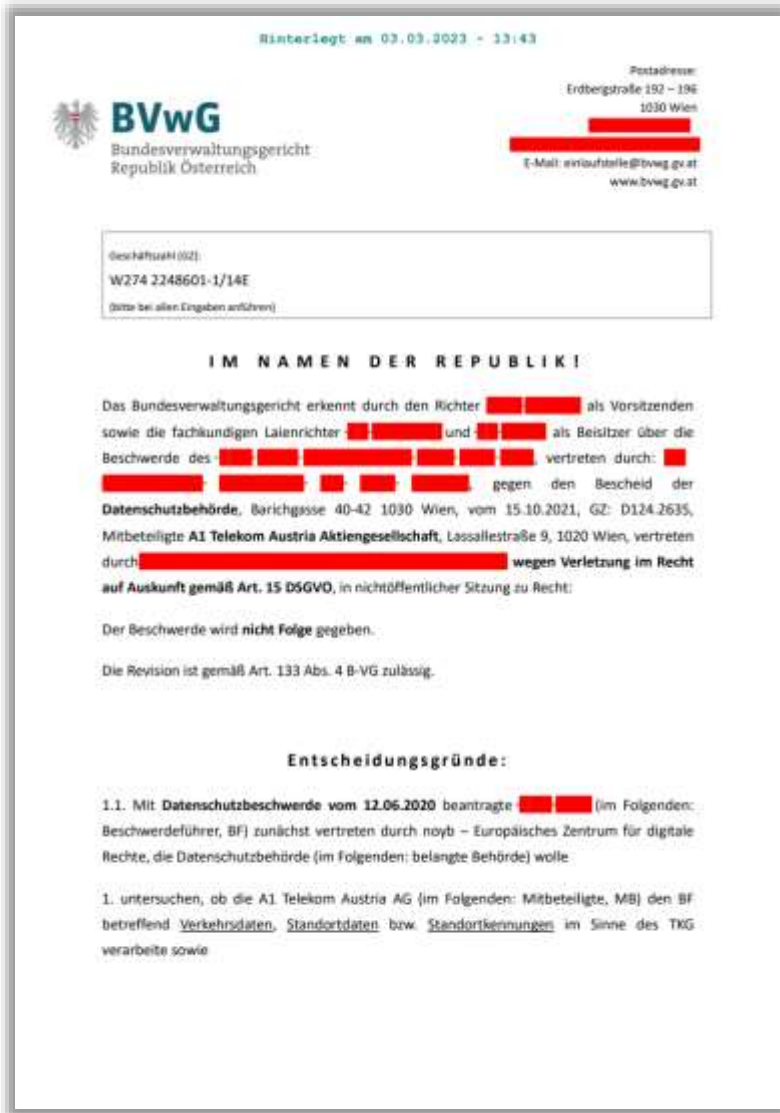
Окружной суд Мюнхена 29.11.2022 вынес решение по иску Федерации немецких организаций потребителей ("vzbz"), запрещающее компании BurdaForward GmbH использовать отслеживающие файлы cookie в рекламных и аналитических целях без действительного согласия потребителей, тем самым частично поддержав иск, поданный vzbz.

BurdaForward, управляющая Интернет-порталом focus.de, использовала cookie-баннер для получения согласия потребителей на хранение cookie и оценку данных, хранящихся на конечных устройствах потребителей, в рекламных и аналитических целях. Баннер предоставлял пользователям возможность выбора: дать полное согласие на обработку их данных и поведения в сети многочисленными сторонними компаниями, нажав на кнопку "Принять все" или сделать альтернативный отдельный выбор, нажав на кнопку "Настройки", при этом появлялось окно с дифференцированными настройками для более чем 100 сторонних компаний на более чем 140 экранных страницах в зависимости от использования данных. Кроме того, кнопки "Принять все" и "Сохранить выбор" были четко выделены, в то время как опция "Отклонить все" была незаметно размещена бледным шрифтом в правом верхнем углу окна.

Суд постановил, что согласие, полученное BurdaForward с помощью баннера, было недействительным, поскольку механизм согласия нарушал применимые правовые требования в соответствии с разделом 25(1) Федерального закона о регулировании защиты данных и конфиденциальности в сфере телекоммуникаций и телемедиа от 23.06.2021 ("TTDSG"), который требует добровольного, информированного и недвусмысленного заявления пользователя о намерениях для того, чтобы согласие было действительным.

Тем не менее, суд отклонил исковое требование vzbz о том, что BurdaForward также должен быть осужден за недостаточную информацию о предполагаемом использовании данных и его соглашения с поставщиками третьих лиц, отметив, что такие информационные обязательства вытекают исключительно из GDPR, а vzbz основывал свои требования исключительно на TTDSG.

## Федеральный административный суд ФРГ отказал субъекту в праве на доступ к геолокационным данным собственного телефона



Клиент A1 Telekom Austria Group направил в компанию запрос информации о трафике и/или данных о местоположении заявителя в соответствии со ст.15 GDPR. Компания ответила, что не может выполнить запрос, поскольку заявитель, как пользователь телефона, не смог в достаточной степени доказать, что он один пользовался телефоном. В связи с этим австрийский орган по защите данных ("DSB") пришел к выводу, что A1 Telekom имела право отказать заявителю в предоставлении данных о трафике, поскольку заявитель не мог быть в достаточной степени идентифицирован.

Так, в договоре между заявителем и компанией не было запрета на передачу, полную или частичную, или эпизодическое использование мобильного устройства другими лицами. Таким образом, A1 Telekom не имел достоверных сведений о фактических пользователях мобильного устройства, и на основании договора не имел полномочий подвергать это использование более тщательной проверке.

Федеральный административный суд ("BVwG") в своем постановлении от 03.03.2023 оставил в силе решение DSB. Заявитель подаст апелляцию на это решение.

## 1107 Голландский суд признал, что Facebook нарушал права пользователей

Окружной суд Амстердама признал, что социальная сеть Facebook нарушала закон о неприкосновенности личной жизни, соответствующее решение опубликовано в среду на сайте инстанции. Теперь пострадавшие смогут требовать компенсации.

Как отмечается в документе, нарушения закона имели место в 2010-2020 годах. "Персональные данные пользователей обрабатывались в рекламных целях, в то время как в данном случае это было запрещено, - подчеркнули судьи. - Персональные данные также передавались третьим лицам без надлежащего информирования пользователей об этом и без наличия для этого оснований в законодательстве и нормативных актах".

Процесс был инициирован Ассоциацией потребителей и Фондом защиты личных данных в 2020 году. Иск был подан от лица более 190 тыс. человек. "Мы очень довольны решением, - отметил представитель Ассоциации потребителей Джерард Спиренбург, чьи слова приводит Нидерландская телерадиовещательная корпорация. - Это очень важный сигнал, причем не только Facebook, но и другим компаниям, что закон о неприкосновенности личной жизни нарушать нельзя".

Компенсация не предусмотрена этим решением, однако является конечной целью истцов. Признание судом, что Facebook нарушил закон, открывает путь к требованию выплат.

Ассоциацией потребителей рассматривается возможность начала переговоров с социальной сетью, но не исключает и подачи иска, к которому по-прежнему могут присоединиться все желающие. "Все зависит от Facebook, - подчеркнул Спиренбург. - Если они не хотят переговоров, мы инициируем новый процесс на основе данного решения". В свою очередь представители корпорации Meta заявили, что намерены подать апелляцию.

## Австрийский суд: раскрытие алгоритма или формулы расчета «маркетинговых классификаций» не является необходимым при ответе на DSAR

Субъект данных обратился с запросом о доступе (DSAR) к контроллеру - поставщику почтовых услуг. Контроллер доставлял целевую политическую рекламу и субъекту данных, почему они были отнесены к определенным политическим симпатиям. Однако, по мнению субъекта данных, ответ контроллера был неполным. Например, в нем не были указаны источники данных и то, каким образом субъект данных был отнесен к определенным политическим предпочтениям для целей политической рекламы.

Субъект данных подал жалобу в австрийский надзорный орган (DPA). Австрийский DPA поддержал жалобу и установил нарушение ст. 12(1) и 15(1)(g) и (h) GDPR, поскольку контроллер не предоставил информацию об источниках данных и о том, каким образом была установлена связь между субъектом данных и определенными политическими группами.

Контролер обжаловал решение, утверждая, что информация, запрошенная субъектом данных, не является персональными данными, а представляет собой лишь "маркетинговые классификации", к которым не применимо ни профилирование в смысле GDPR, ни ст.22(1) GDPR.

Федеральный административный суд Австрии (Bundesverwaltungsgericht - "BVwG") поддержал апелляцию контролера.

Во-первых, по мнению судей, источники были должным образом раскрыты в ответе на запрос о доступе. Кроме того, раскрытие информации было прозрачным и понятным, что соответствовало требованиям ст.12(1) GDPR.

Во-вторых, что касается предполагаемого нарушения ст.15(1)(h) GDPR, суд установил, что контролер предоставил достаточную информацию для понимания логики автоматизированного принятия решений в соответствии со ст. 22(1) и (4) GDPR. По сути, обрабатывались такие данные, как адрес, возраст и пол субъекта данных; использовался "статистический" метод; целью обработки было избежать доставки субъекту данных нерелевантной рекламы. Суд не стал рассматривать вопрос о том, является ли данная обработка профилированием, а также вопрос о том, являются ли "маркетинговые классификации" персональными данными. Суд указал, что раскрытие алгоритма или формулы расчета не является необходимым в соответствии со ст. 15(1)(h) GDPR.

Таким образом, суд отменил решение DPA и заявил, что нарушения ст. 12 и 15 GDPR не было.

[https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT\\_20230612\\_W252\\_2237416\\_1\\_00/BVWGT\\_20230612\\_W252\\_2237416\\_1\\_00.html](https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20230612_W252_2237416_1_00/BVWGT_20230612_W252_2237416_1_00.html)

[https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT\\_20230612\\_W252\\_2237416\\_1\\_00/BVWGT\\_20230612\\_W252\\_2237416\\_1\\_00.pdf](https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20230612_W252_2237416_1_00/BVWGT_20230612_W252_2237416_1_00.pdf)

Также см. аналогичный кейс [https://gdprhub.eu/index.php?title=BVwG\\_-\\_W252\\_2246581-1/6E](https://gdprhub.eu/index.php?title=BVwG_-_W252_2246581-1/6E)

## Австрийский суд: создание учетной записи для покупки товаров на сайте может быть обусловлено согласием на рекламу при условии наличия альтернативы

Субъект данных создал учетную запись у контроллера с целью приобретения товаров в Интернете. В связи с этим он якобы был вынужден дать согласие на обработку своих персональных данных в целях рекламы. Субъект данных подал жалобу в австрийский надзорный орган (DPA). Австрийский DPA признал обработку незаконной.

Контролер обжаловал это решение, утверждая, что субъект данных не был фактически "вынужден" создавать учетную запись для приобретения товара. На самом деле он мог заказать товар, воспользовавшись так называемой "гостевой" опцией, что не подразумевало бы никакой обработки в рекламных целях. Напротив, создание учетной записи подразумевает, что пользователь хочет иметь доступ к скидкам и быть информированным о предложениях, касающихся продукции контроллера.

Федеральный административный суд Австрии (Bundesverwaltungsgericht - "BVwG") поддержал апелляцию контроллера.

В соответствии со ст.4(11) GDPR, согласие должно быть свободно выраженным. В свете ст.7(4) GDPR это явно не так, когда заключение договора ставится в зависимость от согласия субъекта данных, если только согласие не является необходимым для исполнения договора.

Таким образом, суд проверил характер договора в рассматриваемом случае. Суд пришел к выводу, что невозможно отделить создание учетной записи у контроллера от покупки товаров в Интернете. Такая учетная запись не служила исключительно для обмена предложениями и скидками с субъектом данных. Покупка товаров скорее может рассматриваться как основной объект договора. Для такой цели согласие на обработку персональных данных в рекламных целях не требовалось.

Затем суд проверил, может ли гостевой вариант быть действительной альтернативой для достижения цели договора. Суд отклонил довод DPA о том, что гостевая опция не является действительной альтернативой созданию учетной записи в отношении покупки онлайн-товаров. Суд признал, что использование гостевой опции влечет за собой дополнительные усилия для пользователя, а именно заполнение полей, которые автоматически заполняются для владельца учетной записи клиента. Однако такие усилия не являются несоразмерными.

В свете вышесказанного суд отменил решение DPA и признал, что согласие на обработку было дано свободно.

## Немецкий суд: инвалид может получить доступ к своим данным в формате, соответствующем его состоянию, даже при условии снижения мер защиты

Субъект данных обратился с запросом на доступ в администрацию социального обеспечения в соответствии с немецким административным правом. Поскольку субъект данных незрячий, он использовал специальное программное обеспечение для чтения цифровых документов. Таким образом, субъект запросил свои персональные данные в формате pdf, поскольку это был единственный формат, совместимый с таким программным обеспечением.

Это потребовало от контролера отправки соответствующих документов по незашифрованной электронной почте. Контролер отказался это сделать, сославшись на соображения безопасности данных, особенно учитывая, что передача касалась медицинских данных.

Контролер предложил субъекту данных создать учетную запись у провайдера услуг электронной почты, позволяющую отправлять зашифрованные сообщения. Субъект данных возразил, что такое решение является дорогостоящим и, учитывая физическое состояние субъекта данных, представляет собой дополнительное препятствие для доступа. Контроллер также предложил другие каналы связи, такие как обычная почта или доступ к определенным услугам на сайте контроллера. К сожалению, ни один из этих вариантов не был жизнеспособной альтернативой для субъекта данных, поскольку его программное обеспечение не могло читать форматы, предлагаемые контроллером.

Социальный суд Гамбурга (Sozialgericht Hamburg - SG Hamburg) удовлетворил иск субъекта данных. По мнению суда, опасения контроллера по поводу безопасности данных были необоснованными. Фактически, субъект данных дал согласие на обработку и даже прямо попросил об этом в соответствии со ст.6(1)(a) GDPR.

Контролер также не мог использовать статью 32(1) GDPR для отказа от выполнения запроса. По мнению суда, лишь потенциальные риски, связанные с безопасностью связи между контроллером и субъектом данных, не могут отменить заинтересованность последнего в том, чтобы не подвергаться дискриминации.

Суд также проанализировал выводы Федерального ведомства по защите персональных данных Германии о возможности отступления от требований технических и организационных мер в соответствии со ст.32 GDPR. Так, для возможности отступления должны быть выполнены три основных требования: во-первых, запрос на менее защитные меры должен исходить от субъекта данных; во-вторых, должны быть конкретные причины, по которым запрашивается отступление; в-третьих, отступление

## Немецкий суд: запрос на доступ к данным будет "чрезмерным" и "неправомерным", если цель не связана с защитой данных

⚖️ Немецкий суд признал запрос на доступ "чрезмерным" и "неправомерным" в соответствии со ст.12(5)(b) GDPR, поскольку его цель не была строго связана с защитой данных, а затрагивала другие права и интересы субъекта данных.

◇ Субъект данных и контролер - страховая компания - вели гражданское разбирательство, касающееся увеличения взносов, которые субъект данных должен был выплачивать для страхования у контролера. Субъект данных утверждал, что такое увеличение было неправомерным. Чтобы доказать это, субъект данных запросил доступ к своим персональным данным в соответствии со ст.15 GDPR. Контроллер отказал в доступе. В связи с этим субъект данных обратился в Региональный суд Гамбурга (Landgericht Hamburg) с просьбой обязать контролера предоставить доступ к информации, о которой идет речь. Суд вынес решение по запросу о предоставлении доступа в контексте более широкого гражданского процесса, ведущегося между сторонами.

◇ Суд отклонил требование субъекта данных. Суд установил, что контролер мог отказаться рассматривать запрос субъекта данных на доступ к информации в соответствии со ст.12(5)(b) GDPR. По сути, запрос был "чрезмерным" и мог быть квалифицирован как случай злоупотребления правом. По мнению суда, цель ст.15 GDPR выражена в п.63 преамбулы GDPR, где четко указано, что запрос на доступ должен позволить субъекту данных узнать об обработке его данных и проверить законность операций по обработке. В данном случае субъект данных пытался воспользоваться ст.15 GDPR с целью, которая не имела никакого отношения к защите данных. Спор между субъектом данных и контролером в действительности был лишь спором по страховому праву.

## Немецкий суд: утрата контроля над персональными данными сама по себе не является основанием для возмещения нематериального ущерба согласно ст.82 GDPR

◇ Субъект данных являлся пользователем Facebook. В соответствии с настройками конфиденциальности, выбранными на момент совершения факта, номер его телефона мог быть использован третьим лицом для поиска профиля субъекта данных в Facebook, даже если сам номер телефона не был публичным. Соответственно, информация, касающаяся субъекта данных, может быть связана с его номером телефона любым лицом, обладающим таким номером.

◇ В 2021 году неизвестные "третьи лица" автоматически комбинировали телефонные номера и сопоставляли их с профилями в Facebook благодаря вышеупомянутой функции. Таким образом, телефонные номера могли быть присвоены идентифицированным пользователям. В результате произошла утечка данных, касающихся 533 млн. человек в 106 различных странах.

◇ Субъекты данных жаловались, что после утечки им стали поступать фишинговые электронные письма и звонки. В связи с потерей контроля над своими персональными данными субъект данных потребовал возмещения ущерба в соответствии со статьей 82 GDPR.

◇ Суд первой инстанции отклонил иск субъекта данных. Субъект данных обжаловал это решение в Высшем региональном суде Хамма (Oberlandesgericht Hamm). Суд оставил в силе решение первой инстанции и разъяснил, что для подачи иска по статье 82 GDPR требуется наличие трех необходимых элементов: нарушение одного из положений GDPR, фактический ущерб, нанесенный субъекту данных, и причинно-следственная связь между нарушением и ущербом.

◇ Что касается первого элемента, то суд предварительно указал на тот факт, что бремя доказывания отсутствия нарушения лежит на контролере. Такой вывод можно сделать на основании ст. 5(2) GDPR, которая возлагает на контролера обязанность доказывать соблюдение GDPR. Контроллер нарушил статью 6 GDPR. Кроме того, суд установил нарушение принципа конфиденциальности по умолчанию (ст. 25(2) GDPR) и общее отсутствие надлежащих мер безопасности для предотвращения скраппинга (ст. 32 GDPR).

◇ Однако второй элемент - наличие реального ущерба - суд посчитал неудовлетворительным. Что касается ущерба, а также причинно-следственной связи, то бремя доказывания лежит на субъекте данных. Предварительно суд сослался на решение CJEU по делу C-300/21 и пояснил, что для компенсации нематериального ущерба не требуется соблюдения какого-либо минимального порога серьезности. Тем не менее, по мнению CJEU, ущерб должен быть "фактическим и определенным" и четко отграниченным от нарушения, из которого он вытекает.



## Австрийский суд: банк, записывающий все звонки клиентов, не может ссылаться на законный интерес

Субъект данных подал жалобу, утверждая, что контроллер (банк) записывает его телефонные разговоры и не имеет возможности отказаться от такой обработки. Клиенты были проинформированы о записи с помощью магнитофонного объявления в начале разговора.

Контроллер обосновал обработку законными интересами в соответствии со Статьей 6(1)(f) GDPR, заявив, что запись необходима для обеспечения наилучшего качества обслуживания клиентов. Контроллер также ссылался на свои обязательства по законодательству ЕС, в частности на Директиву 2014/65/EU (MiFID II), и на национальное банковское законодательство, в частности на § 66(1) Закона о платежных услугах (Zahlungsdienstegesetz - ZaDiG) и § 33(2) и (3) Закона о надзоре за ценными бумагами 2018 года (Wertpapieraufsichtsgesetz 2018 - WAG).

Австрийский DPA удовлетворил иск субъекта данных и вынес решение против контроллера. Контроллер обжаловал это решение в Федеральном административном суде Австрии (Bundesverwaltungsgericht). К приведенным выше аргументам контроллер добавил, что невозможно не записывать все входящие звонки. Кроме того, контроллер поставил под сомнение компетенцию DPA, поскольку дело якобы подпадало под действие WAG, а не GDPR.

Суд отклонил апелляцию контроллера и подтвердил компетентность DPA. Жалоба субъекта данных касалась его права на конфиденциальность персональных данных. Нарушение ст. 6(1) GDPR может привести к нарушению § 1(1) австрийского Закона о защите данных (Datenschutzgesetz - DSG), который содержит фундаментальное право на защиту данных. Право на конфиденциальность входит в компетенцию DPA.

Что касается законного интереса, то суд указал на то, что интерес контроллера "обеспечить качество" не был дополнительно объяснен контроллером. Поэтому статья 6(1)(f) GDPR не может быть использована в качестве законного основания. Аргумент контроллера о сложности/невозможности записи не всех звонков также был отклонен судом. По сути, контроллер обязан разработать внутренние процедуры таким образом, чтобы положения, вытекающие из банковских правил, не противоречили положениям о защите данных. В § 33 (2) и (3) WAG определено, какие звонки должны записываться определенными юридическими лицами, включая банки. Данное положение гласит, что записываться должны только звонки, связанные с инвестиционными услугами. Таким образом, суд исходил из того, что речь идет об инвестиционных услугах, когда речь идет об обязанности записывать телефонные разговоры.

Суд указал, что тема входящего телефонного звонка может быть выяснена в начале разговора. Телефонные разговоры, не касающиеся инвестиционных услуг, не подлежат записи. В данном случае субъект данных хотел получить лишь общую информацию. Никаких признаков отношения к инвестиционным услугам не было. Таким образом, § 33(2) и (3) WAG неприменим, а обработка данных является незаконной.

## Федеральный административный суд Австрии постановил, что субъекты данных не могут добиваться назначения DPO

◇ Федеральный административный суд (BVwG) в своем решении от 03.08.2023 г. частично подтвердил решение австрийского органа по защите данных (DSB), касающееся права доступа, права на неприкосновенность частной жизни и права требовать назначения ответственного за защиту данных (DPO) заявителя в соответствии с GDPR.

◇ По словам заявителя, его право на доступ было нарушено ответчиком - неназванным университетом. Университет направил электронное письмо о предполагаемом нарушении заявителем своих служебных обязанностей в несколько департаментов. Кроме того, когда заявитель запросил доступ к своим данным, он получил документ объемом более 800 страниц, в котором не было ни одной ссылки на него. Кроме того, BVwG заявила, что, по мнению заявителя, ответ на запрос о доступе должен был дать DPO, а не декан университета.

◇ Суд установил, что университет нарушил право заявителя на конфиденциальность, отправив вышеупомянутое электронное письмо и письмо, которое было раскрыто другим лицам. В отношении рассмотрения вопроса о назначении DPO, суд постановил, что, хотя назначение DPO представляет собой обязанность контроллера данных, оно не влечет за собой права субъекта данных требовать назначения DPO. В свете вышеизложенного BVwG частично удовлетворил жалобу и отклонил апелляцию.

## Высший административный суд земли Рейнланд-Пфальц постановил, что владелец автомобиля обязан раскрывать личность водителя при расследовании нарушения ПДД

Владельцем автомобиля выступала неназванная компания (далее - контролер), которая разрешала своим сотрудникам пользоваться служебным автомобилем. Один из таких автомобилей был использован для совершения нарушений правил дорожного движения. В ходе полицейского расследования не было установлено, кто из сотрудников управлял автомобилем в тот момент. Поэтому компетентная администрация потребовала от контролера раскрыть личность водителя.

Кроме того, администрация обязала контролера вести журнал учета своих автомобилей, лиц, которым они были предоставлены, и других сведений, касающихся услуг, предлагаемых контролером. Правовое основание для такого обязательства содержится в немецком законодательстве о дорожном движении. Контролер отказался выполнять предписание и обжаловал его в суде. Контролер утверждал, что GDPR не позволяет раскрывать персональные данные водителя (водителей) властям и вести журнал учета с именами водителей.

Суд первой инстанции отклонил иск, и контролер обжаловал решение в Высшем административном суде земли Рейнланд-Пфальц (Oberverwaltungsgericht Rheinland-Pfalz, OVG Rheinland-Pfalz). Апелляционный суд оставил в силе решение первой инстанции. По мнению суда, как раскрытие персональных данных водителей, так и ведение журнала с персональными данными последних было допустимо в соответствии со ст.6(1)(f) GDPR. В качестве правового основания контролер мог (и должен был) полагаться на защиту законных интересов органов власти при выполнении задач, возложенных на них в общественных интересах, которые включают в себя преследование за административные правонарушения. Кроме того, суд отметил, что дальнейшие этапы обработки были также разрешены со стороны государственного органа в соответствии со ст.6(1)(e) GDPR.

## Высший суд Любляны постановил, что права на частную собственность должны превалировать над правом на неприкосновенность частной жизни

Высший суд Любляны (Višje sodišče v Ljubljani) отклонил апелляцию, поданную субъектом данных (признанным виновным в хищении денег из банкомата) о том, что запись камер видеонаблюдения банкомата не может быть признана допустимым доказательством, поскольку отсутствовало предупреждение о видеонаблюдении.

Выводы суда:

- ◇ право на неприкосновенность частной жизни не является абсолютным, оно может быть ограничено, например, правами других лиц и в предусмотренных законом случаях;
- ◇ камеры вели съемку зоны перед банкоматом, где человек не может рассчитывать на уединение в абсолютном смысле, т.е. право обвиняемого на неприкосновенность частной жизни не было нарушено в несоразмерной степени;
- ◇ даже если бы камеры наблюдения не были достаточно заметны или не сопровождалась достаточно заметными предупреждениями, они не являлись бы недопустимым доказательством;
- ◇ возможное отсутствие уведомления о видеонаблюдении не носит настолько серьезного характера, чтобы обоснованно привести к различному восприятию общественного пространства лицами, находящимися вблизи промышленных зон, предприятий, дорог общего пользования, банкоматов и т.д.;
- ◇ права пострадавшей компании на ее частную собственность должны превалировать над правом субъекта данных на неприкосновенность частной жизни в момент совершения правонарушения, поскольку в противном случае потенциальные преступники могли бы беспрепятственно совершать свои правонарушения.

## Административный суд Берлина: оператор поездов может не предоставлять записи видеонаблюдения пассажирам

Поезда сети берлинских поездов S-Bahn оборудованы камерами видеонаблюдения, записанные данные сохраняются в течение 48 часов, а затем автоматически удаляются, если только их не затребуют правоохранительные органы. Субъект данных совершил поездку на поезде 6 октября 2020 года и в тот же день отправил электронное письмо оператору сети поездов (контролеру данных) с просьбой предоставить доступ к записям камер видеонаблюдения в поезде, в котором она ехала, и попросил не удалять записи автоматически через 48 часов. Контролер отказался это сделать, поскольку, он может предоставлять такие данные только правоохранительным органам.

Административный суд Берлина (Verwaltungsgericht Berlin - VG Berlin) постановил, что контролер не обязан предоставлять субъекту данных видеозаписи камер видеонаблюдения, о которых идет речь. Суд признал, что содержащиеся в них данные представляют собой персональные данные в соответствии со статьей 4(1) GDPR, поскольку лица могут быть идентифицированы, а также потому, что в соответствии со статьей 11 GDPR идентификация лиц в момент обработки не является обязательной. Однако суд добавил, что необходимо принимать во внимание фактическую способность истца идентифицировать лицо, и пришел к выводу, что в данном конкретном случае истец не располагал средствами, необходимыми для фактической идентификации субъекта данных, поэтому Berlin VG постановил, что видеозаписи истца не содержат никаких персональных данных и должны рассматриваться как обезличенные данные.

Во-вторых, суд постановил, что даже при наличии информации, предоставленной субъектом данных: даты, номера поезда и других данных, истец не мог быть уверен, что субъект данных является именно тем лицом, которое подает запрос на доступ, поскольку он мог предоставить эту информацию, но в отношении другого лица. Истец может установить личность только с помощью информации, предоставленной правоохранительными органами в случае запроса на доступ к записям. Кроме того, суд решил, что усилия, которые потребовались истцу для проверки и обезличивания данных, были совершенно непропорциональны заинтересованности субъекта данных в этой информации. Все это, по мнению суда, сделало запрос на доступ чрезмерным.

Несмотря на то, что статья 15 GDPR не предусматривает исключений в случае несоразмерных запросов на доступ, суд постановил, что это можно сделать на основании толкования § 275(2) Гражданского кодекса Германии (Bürgerliches Gesetzbuch - BGB) и примечания 62 GDPR. Из толкования суда следует, что в исполнении может быть отказано, если это требует несоразмерных усилий, которые, согласно принципу добросовестности, предусмотренному в статье 8(2) Хартии и статье 5(1)(a) GDPR, преобладают над интересами субъекта данных.

Кроме того, суд подчеркнул, что автоматическое удаление записей через 48 часов, которое служит для защиты интересов всех других лиц, запечатленных в ходе видеонаблюдения, и которое предусмотрено законом, перекрывает интересы субъекта данных в получении доступа к такой информации. Субъект данных также не может опираться на Статью 17(3)(b) GDPR и Статью 18(1)(c) GDPR для предотвращения автоматического удаления записей, поскольку право на доступ в соответствии со Статьей 15 GDPR не предусмотрено в них.

<https://gesetze.berlin.de/perma?d=JURE230058334>

[https://gdprhub.eu/index.php?title=VG\\_Berlin\\_-\\_1\\_K\\_561/21](https://gdprhub.eu/index.php?title=VG_Berlin_-_1_K_561/21)

## 1118 Суд обязал LinkedIn соблюдать GDPR и не игнорировать «do-not-track»



**Gericht untersagt Datenschutzverstöße von LinkedIn**  
Landgericht Berlin gibt Klage des vzbv gegen die LinkedIn Ireland Unlimited Company weitgehend

- LinkedIn teilte Nutzer:innen auf der Webseite mit, dass auf im Browser eingestellte „Do-Not-Track“-Signale derzeit nicht reagiert wird.
- Voreinstellung zur Sichtbarkeit der Mitgliederprofile auf Partnerseiten des Unternehmens ist unzulässig.
- In einem Teilurteil hatte das LG Berlin zuvor bereits den ungebetenen Versand von E-Mails an Nichtmitglieder verboten.

Das soziale Netzwerk LinkedIn darf auf seiner Webseite nicht mehr mitteilen, dass es auf „Do-Not-Track“-Signale nicht reagiert, mit denen Nutzer:innen der Nachverfolgung („Tracking“) ihres Surfverhaltens per Browsereinstellung widersprechen. Das hat das Landgericht Berlin nach einer Klage des Verbraucherzentrale Bundesverbands (vzbv) entschieden. Das Gericht untersagte dem Unternehmen außerdem eine Voreinstellung, nach der das Profil des Mitglieds auch auf anderen Webseiten und Anwendungen sichtbar ist. Bereits im vergangenen Jahr hatte das Gericht den ungebetenen Versand von E-Mails an Nichtmitglieder untersagt.

Региональный суд Берлина (Landgericht Berlin) в целом удовлетворил иск Федерации немецких потребительских организаций (vzbv) к компании LinkedIn Ireland Unlimited о прекращении неправомерной обработки персональных данных и игнорировании сигналов DNT.

◇ LinkedIn ранее игнорировала сигналы DNT (do-not-track, не отслеживать) от пользователей, которые заходят в свои аккаунты через браузеры. С помощью этих сигналов человек может запретить отслеживание своих действий на сайте. На справочной странице LinkedIn размещено [предупреждение](#) о том, что платформа не берет DNT во внимание. Суд обязал разработчиков убраться от этого заявления.

◇ Немецкие судьи запретили LinkedIn включать публичный доступ ко всем аккаунтам по умолчанию. Ранее эта настройка делала личные страницы доступными для поисковиков и незарегистрированных посетителей без согласия владельцев.

◇ Суд также запретил LinkedIn собирать персональные сведения, такие как IP-адреса, в аналитических и маркетинговых целях, в том числе предоставлять доступ к этим базам третьим лицам, без согласия подписчиков.

## Региональный суд Мюнстера: интересы субъекта-банкрота приоритет над интересами кредитного агентства

Субъект данных столкнулся с процедурой банкротства, о которой было объявлено в общедоступной базе данных. Согласно немецкому законодательству, эта публикация сохраняется и становится общедоступной в течение 6 месяцев после процедуры банкротства. Кредитное агентство (контролер) негативно зарегистрировало субъекта данных, используя информацию из общедоступной базы данных, и передало негативную информацию о субъекте данных своим партнерам по договору. В результате субъект данных не смог подать заявку на получение кредитных продуктов.

Получив отказ по различным кредитным заявкам в связи с отрицательной репутацией, субъект данных подал иск против кредитного агентства в Региональный суд Мюнстера (LG Münster). Суд постановил, что контролер нарушил ст.6(1) GDPR, поскольку у него не было законного основания для обработки данных субъекта. Суд постановил, что контролер не мог сослаться на ст.6(1)(f) GDPR для обработки данных, поскольку экономические интересы контролера не могли преобладать над интересами субъекта данных. Более того, контролер хранил информацию о несостоятельности субъекта данных дольше 6-месячного срока, предусмотренного внутренним законодательством.

Интересы и права субъекта данных имеют приоритет над интересами и правами контролера. Негативная информация нанесла неоправданный ущерб экономической жизни субъекта данных. Суд пришел к выводу, что обработка данных контролером существенно нарушила конституционное право субъекта данных на самоопределение в соответствии со статьями 1,2 Основного закона Германии, право на защиту данных в соответствии со статьей 8 Европейской хартии основных прав, а также общую свободу действий, свободу договора и свободу профессиональной деятельности субъекта данных. В результате суд обязал контролера стереть персональные данные субъекта данных в соответствии со ст.17(1)(d) GDPR и выплатить субъекту данных 579,17 евро в качестве компенсации ущерба в соответствии со ст.82(1) GDPR.

## Административный суд Австрии: автоматическая блокировка электронной почты – это не автоматизированное решение

◇ Субъект данных в Австрии установил на входной двери своего дома камеру, предоставленную поставщиком телекоммуникационных услуг (контролером данных). Заметив, что больше не получает уведомлений по электронной почте от камеры на входной двери, он обратился к контролеру и в разных случаях получил различную и противоречивую информацию о причинах сбоев в работе системы. Позже субъект данных узнал, что его учетная запись была автоматически заблокирована, а контролер ответил, что это произошло из-за ненадлежащего использования учетной записи.

◇ Субъект данных жалобу в австрийский надзорный орган (DSB), а позднее – иск в Федеральный административный суд Австрии (Bundesverwaltungsgericht - BVwG), в связи с предполагаемой утечкой своих данных и незаконным автоматизированным принятием решения контролером.

◇ BVwG постановил, что блокировка учетной записи электронной почты заявителя была установлена алгоритмом в связи с необычно высокой активностью в качестве меры по борьбе со спамом. Так, контролер заявил, что заметил большое количество электронных писем, отправленных с учетной записи субъекта данных в течение короткого периода времени, и заподозрил неправомерное использование его учетной записи.

◇ BVwG решил, что блокировка учетной записи электронной почты алгоритмом не может считаться автоматизированным решением, оказывающим юридическое или аналогичное значительное воздействие на субъекта данных в соответствии со ст.22(1) GDPR. По мнению BVwG, это техническая и организационная мера по обеспечению безопасности данных и целостности сети, принятая контролером, и, следовательно, разрешенная в соответствии со статьей 22(2)(a) GDPR, как необходимая для исполнения договора между ними.



# Влияние GDPR на бизнес



## Исход американского СМБ из европейского рынка по причине неготовности к выполнению требований GDPR

- ❖ [Brent Ozar](#), IT consulting services
- ❖ [CoinTouch](#), peer-to-peer cryptocurrency exchange
- ❖ [Drawbridge](#), cross-device identity service
- ❖ [FamilyTreeDNA](#), free and public genetic tools such as Mitosearch and Ysearch
- ❖ [Gravity Interactive](#), video game developer (Ragnarok Online, Dragon Saga)
- ❖ [Hitman: Absolution](#), video game developed by IO Interactive
- ❖ [Klout](#), social reputation service by Lithium
- ❖ [Loadout](#), video game developed by Edge of Reality
- ❖ [Monal](#), XMPP chat app
- ❖ [MotoSport](#), powersports retailer
- ❖ [Parity](#), know-your-customer service for initial coin offerings (ICOs)
- ❖ [Payver](#), dashcam app
- ❖ [Pottery Barn](#), housewares retailer
- ❖ [Seznam](#), social network for students
- ❖ [Steel Root](#), cybersecurity and IT services
- ❖ [StreetLend](#), tool sharing platform for neighbors
- ❖ [Super Monday Night Combat](#) (SMNC), video game developed by Uber Entertainment
- ❖ [Tungle](#), video game VPN
- ❖ [Unroll.me](#), inbox management app
- ❖ [Verve](#), mobile programmatic advertising
- ❖ [Williams-Sonoma](#), housewares retailer

## Капитализация Facebook за один день упала на рекордные для рынка США \$120 млрд

Это произошло на фоне отчета о о предстоящем замедлении тем регулятивного давления

Facebook Inc., как стало известно в четверг, во втором квартале увеличила чистую прибыль на 31%, но она не дотянула до прогнозов рынка. Выручка подскочила на 42% и достигла \$13,231 млрд.

Однако руководство Facebook предупредило, что темпы роста будут замедляться: в частности, из-за замедления роста рекламных доходов подъем выручки во втором квартале в годовом выражении был на 7 процентных пунктов меньше, чем в первом квартале, и эта тенденция сохранится во втором полугодии.

Кроме того, компания ожидает более быстрого увеличения расходов в 2019 году из-за, в частности, различных регулятивных рисков. В результате следующие несколько лет будет в районе 35%, в то время как во втором

Из-за введения в Европе нового законодательства о защите персональных данных число активных пользователей Facebook в регионе упало за квартал на 1%.

Facebook столкнулась также с последствиями скандала вокруг Cambridge Analytica, который потребовал от сети увеличения внимания к защите данных пользователей.

## The Guardian

Global development Football Tech Business Environment Obituaries

### Facebook moves 1.5bn users out of reach of new European privacy law

Facebook has moved more than 1.5 billion users out of reach of European privacy law, despite a promise from Mark Zuckerberg to apply the “spirit” of the legislation globally.


In a tweak to its terms and conditions, Facebook is shifting the responsibility for all users outside the US, Canada and the EU from its international HQ in Ireland to its main offices in California. It means that those users will now be on a site governed by US law rather than Irish law.

<https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law>

TechGenYZ TG NOW TECH FUTURE GAMING HOW TO PHONE FINDER DEALS REVIEWS

### Seven European Union countries accuse Google of GDPR violations

By Dindhi Banerjee  
Nov 27, 2018, 4:30 Pm



Consumer groups from seven European countries, including Poland and Netherlands, have filed GDPR complaints against Google's location tracking which is in violation of the bloc's new privacy laws. Members of The European Consumer Organisation (BEUC), each of the countries claim that Google's 'deceptive practices' around location tracking deprive users of exercising a real choice about enabling it, while Google fails to, at the same time, properly inform users about what the tracking entails. If upheld, the complaints could lead to Google having to pay a hefty fine. Google is facing a similar charge in the US, where the search engine giant has been accused of tracking phone users irrespective of privacy settings.

The consumer groups, in the Czech Republic, Greece, Norway, Slovenia, and Sweden, have each filed complaints with their respective national data protection authorities. reports a research by their Norwegian counterpart, Consumer lobby the European Consumer Organisation (BEUC) have alleged that Google uses various methods to encourage users to enable the settings 'location history' and 'web and app activity' integrated into all Google user accounts.

Участники Европейской потребительской организации - Bureau Européen des Unions de Consommateurs (BEUC) из семи европейских стран (Польши, Нидерландов, Чехии, Греции, Норвегии, Словении и Швеции) обвинили Google в нарушении требований GDPR и подали жалобы в соответствующие национальные органы по защите данных (DPA). BEUC утверждает, что Google использует различные недобросовестные практики, чтобы мотивировать пользователей включать в веб-браузере и мобильных приложениях опцию отслеживания местоположения пользователя, интегрированную во все пользовательские учетные записи Google.

## Против авиакомпании EasyJet подан коллективный иск на 18 миллиардов фунтов из-за утечки данных

**ZDNet**

### EasyJet faces £18 billion class-action lawsuit over data breach

The lawsuit aims to secure up to £2,000 per impacted customer.

By [Charlie Osborne](#) for [Zero Day](#) | May 26, 2020 -- 10:38 GMT (03:38 PDT) | Topic: [Security](#)

**You'll need more than an antivirus: 'Malware-free' attacks on the rise**  
0:48  
[WATCH NOW](#)

UK budget airline easyJet is facing an £18 billion class-action lawsuit filed on behalf of customers impacted by a recently-disclosed data breach.

Made public on May 19, easyJet said that information belonging to [nine million customers](#) may have been exposed in a cyberattack, including over 2,200 credit card records.

The "highly sophisticated" attacker to blame for the security incident managed to access this financial information, as well as email addresses and travel details. EasyJet is still contacting impacted travelers.

**SECURITY**

- [Windows 10 to get PUA/PUP protection feature](#)
- [Best security keys in 2020: Hardware-based two-factor authentication for online protection](#)
- [Best password managers](#)

Бюджетная британская авиакомпания EasyJet столкнулась с коллективным иском в 18 миллиардов фунтов стерлингов, поданным в мае 2020 года от имени клиентов, пострадавших от недавно обнаруженной утечки данных. Речь идет о персональных данных девяти миллионов клиентов, которые были раскрыты в результате успешной кибератаки, включая более 2,200 записей о кредитных картах.

Сам иск был подан в Высокий суд Лондона юридической фирмой PGMBM, представляющей интересы пострадавших клиентов EasyJet. Требования о компенсации в размере 2,000 фунтов на каждого из клиентов основаны на ст.82 GDPR. По данным фирмы, утечка данных произошла в январе 2020 года, и, хотя ICO (британский надзорный орган), по-видимому, была своевременно уведомлена об этом, но сами клиенты так и не были официально оповещены авиакомпанией об инциденте даже спустя четыре месяца.

## Профессиональные футболисты угрожают спортивным дата-брокерам судебным иском GDPR



**BBC**

### NEWS

# Professional footballers threaten data firms with GDPR legal action

By Nick Hartley  
BBC Wales News

12 October 2021

**Hundreds of footballers have threatened legal action against the data collection industry, which could change how information is handled.**

Led by former Cardiff City, Leyton Orient and Yeovil Town manager Russell Slade, 850 players want compensation for the trading of their performance data over the past six years.

They also want an annual fee from the companies for any future use.

"Letters before action" have been sent to 17 big firms, alleging data misuse.

Data ranges from average goals-per-game for an outfield player to height - however, Mr Slade **has previously expressed concern** this is sometimes wrong.

If the group pursues legal action and is successful, it could lead to a radical change of a multi-billion pound industry behind professional sport that trades on players' information.

Slade's legal team said the fact players receive no payment for the unlicensed use of their data contravenes General Data Protection Regulation (GDPR) rules that were strengthened in 2018.

Under Article 4 of the GDPR, "personal data" refers to a range of identifiable information, such as physical attributes, location data or physiological information.

BBC News understands that an initial 17 major betting, entertainment and data collection firms have been targeted, but Slade's Global Sports Data and Technology Group has highlighted more than 150 targets it believes have misused data.

В Великобритании группа из 850 профессиональных футболистов хочет судиться со спортивными дата-брокерами - спортсмены требуют, чтобы им платили комиссию за коммерческое использование персональных данных, на которое они не давала своего явного согласия. Соответствующие досудебные уведомления отправили в 17 крупнейших компаний, а всего в неправомерной обработке данных обвиняют 150 организаций.

Причиной иска является то, что аналитики футбольных команд уже давно собирают данные о действиях игроков на поле с помощью умных камер-трекеров. Основываясь на этих данных, команды анализируют производительность игроков, улучшают игровую стратегию и принимают решения о трансферах. Кроме этого, игровые данные продают - аналитическим компаниям, разработчикам игр, букмекерам.

## 1127 Голландские потребители подали иск против Google на €61,5 млн



The image shows a screenshot of a news article from the website Consumentenbond.nl. The page features a search bar at the top with the text 'Waar ben je naar op zoek?' and a magnifying glass icon. To the right of the search bar is the Consumentenbond logo, which includes a blue triangle and the text 'Consumentenbond' and '70 Jaar'. Below the search bar are navigation links: 'Producttests', 'Geldzaken', 'Juridisch Advies', and 'Alle thema's'. The main headline is 'Google voor de rechter gedaagd' in large, bold, dark blue letters. Below the headline is a sub-headline in smaller text: 'Nieuws | De Stichting Bescherming Privacybelangen en de Consumentenbond zetten de volgende stap in hun strijd tegen Google. Het techbedrijf wordt vandaag voor de rechter gedaagd wegens grootschalige privacyschendingen. In de procedure wordt onder andere geëist dat Google stopt met zijn constante surveillance en het delen van persoonsgegevens via online advertentievervalsingen en daarnaast schadevergoeding betaalt aan consumenten. Sinds de aankondiging van deze actie op 23 mei 2023 hebben al ruim 82.000 Nederlanders zich aangesloten bij de massaclaim.' At the bottom left of the article is a small circular profile picture of a woman, followed by the text 'Babs van der Staak | Woordvoerder' and 'Gepubliceerd op: 12 september 2023'.

Ассоциация потребителей Нидерландов совместно с организацией Фонд по защите конфиденциальности подали судебный иск против компании Google на сумму \$66 млн из-за возможных широкомасштабных нарушений неприкосновенности частной жизни.

Согласно заявлению ассоциации, истцы обвинили корпорацию в "постоянном отслеживании и обмене персональными данными через интернет-рекламные торги". Они потребовали выплаты компенсации в размере €750 каждому, кто "использовал поисковую систему Google".

Иск подан в голландский суд от имени 82 тыс. человек.

<https://tass.ru/ekonomika/18730463>

<https://www.consumentenbond.nl/acties/google-claim>

## 1128 Голландские privacy-энтузиасты подали иск против X Corp. (Twitter) и MoPub

Нидерландская некоммерческая организация по защите данных Stichting Data Bescherming Nederland (SDBN) начала судебные разбирательства против X Corp. (Twitter) и MoPub, платформу для управления и обмена мобильной рекламой MoPub, которая до 1 января 2022 года принадлежала X Corp. Компании обвиняются в незаконной торговле персональными данными миллионов пользователей мобильных приложений.

◇ Иск предъявлен от имени около 10 млн. взрослых и 1 млн. детей в Нидерландах, которые предположительно использовали около 30 000 приложений со встроенными трекерами MoPub, например, игры, приложения для отслеживания менструаций, приложения для знакомств и другие.

◇ В документах по делу утверждается, что данные пользователей собирались и передавались без их ведома или согласия, что является нарушением GDPR. Истцы также требуют, чтобы незаконно собранные данные были удалены.

◇ В пресс-релизе SDBN утверждается, что в период с октября 2013 года по декабрь 2021 года, даже если пользователи никогда не публиковали твиты, бесплатные приложения позволяли X и MoPub собирать и делиться их персональными данными и другими данными, в том числе информацией о сексуальной ориентации, желаниях детей или религиозных убеждениях. Собранные данные затем продавались тысячам сторон.

◇ В SDBN выразили озабоченность тем, что регуляторы до сих пор не смогли эффективно регулировать деятельность в этой области. Представитель организации заявил, что, если нарушение GDPR не станет слишком дорогостоящим, компании продолжат его нарушать.

◇ Если иск удастся выиграть, штрафы могут составить несколько миллиардов евро. Однако окончательное решение по этому делу ожидается не ранее 2026 года.



## 1129 Голландские privacy-энтузиасты подали иск против Adobe

Нидерландская организация по защите данных Stichting Data Bescherming Nederland (SDBN) обвиняет американскую компанию Adobe в незаконном сборе и распространении личных данных миллионов жителей Нидерландов.

◇ Adobe, известная своими программными продуктами для творчества и мультимедиа, обвиняется в тайном сборе данных с посетителей популярных в Нидерландах веб-сайтов и приложений, включая телекоммуникационную KPN, местный пенсионный фонд и налоговую службу. По утверждению SDBN, данные передаются третьим сторонам без согласия пользователей, используя скрытые трекеры и SDK в приложениях.

◇ SDBN утверждает, что это практика нарушает GDPR, подвергая пользователей риску утечек данных, мошенничества и других проблем конфиденциальности. Утверждается, что Adobe собирает данные практически всех граждан Нидерландов, включая тех, кто никогда не пользовался продуктами Adobe.

◇ SDBN требует прекратить скрытое отслеживание и возместить ущерб миллионам пострадавших граждан. Компания подала коллективный иск, требуя от Adobe прекратить незаконный сбор данных, уничтожить уже собранные данные и раскрыть все стороны, которым эти данные разглашались. Иск направлен на прекращение использования трекеров на популярных сайтах и скрытого кода в приложениях, таких как торговая площадка Marktplaats и погодный сервис Buienradar.

◇ Голландские интернет-пользователи могут присоединиться к иску, зарегистрировавшись на сайте SDBN. Анук Рухаак, председатель SDBN, выразила искреннее удивление вовлечённостью Adobe в сбор и торговлю персональными данными.

<https://www.securitylab.ru/news/544601.php>

<https://adobe.iestaattekoop.nl/>

## 1130 Испанские СМИ подали иск против Meta на €550 млн

**ami** Asociación de Medios  
de Información

04/12/2023 / [Noticias](#), [Publicidad digital](#)

### Los medios de información agrupados en AMI demandan a META por competencia desleal y reclaman más de 550 millones




La Asociación de Medios de Información (AMI) ha presentado una demanda contra META, en representación de 83 medios de información españoles, por su sistemático y masivo incumplimiento de la normativa europea de protección de datos durante el periodo comprendido entre el 25 de mayo de 2018 y el 31 de julio de 2023, y ello sin perjuicio de la posible ampliación de la demanda por la persistencia de META en sus incumplimientos según se deriva del requerimiento formulado el pasado 27 de octubre de 2023 por el

◇ Ассоциация AMI, в которую входят 83 испанские медиакорпорации, сообщила 04.12.2023 о подаче иска против корпорации Meta (признана экстремистской и запрещена в РФ). AMI обвиняет ее в нарушении правил честной конкуренции на рекламном рынке и действующих в ЕС норм по защите данных пользователей. Ассоциация требует от Meta компенсации в размере €550 млн. Иск был подан в испанский суд в прошлую пятницу.

◇ В AMI в числе прочих входят такие издания, как El País, El Mundo, ABC, La Vanguardia. По мнению ассоциации, Meta «массово» и «систематически» использует персональные данные, собираемые принадлежащими ей платформами, без согласия пользователей, что дает ей «несправедливое» преимущество на рекламном рынке. По мнению президента AMI Хосе Жоли, Meta достигла доминирующего положения методами, нарушающими законы, а само это положение корпорации на рекламном рынке наносит ущерб испанским СМИ и ставит их существование под угрозу.

◇ Как отметил адвокат Николас Гонсалес-Куэльяр, подобные процессы против Meta могут быть начаты и в других европейских странах, так как речь идет о нарушении законодательства ЕС. В Meta пока никак не прокомментировали обвинения.

## Проблемы компаний «гиг-экономики», связанные с легальностью слежки за своими работниками




### Our letter to gig economy companies about surveillance of their workers

**CONTENT TYPE**  
News & Analysis

**POST DATE**  
13th December 2021

To add your voice to our letter to gig economy companies like Uber, Deliveroo, Bolt, Amazon Flex, Just Eat, Free Now, and Ola, [sign the Managed by Bots petition](#).



To add your voice to the letter below, which we'll be sending to gig economy companies like Uber, Deliveroo, Bolt, Amazon Flex, Just Eat, Free Now, and Ola, [sign the Managed by Bots petition](#)

Worker Info Exchange (WIE), the App Drivers and Couriers Union (ADCU), Privacy International (PI) and other civil society organisations\* are today writing to you with urgent questions about the exploitation of the workers who underpin the success and rapid growth of your innovative tech platform.

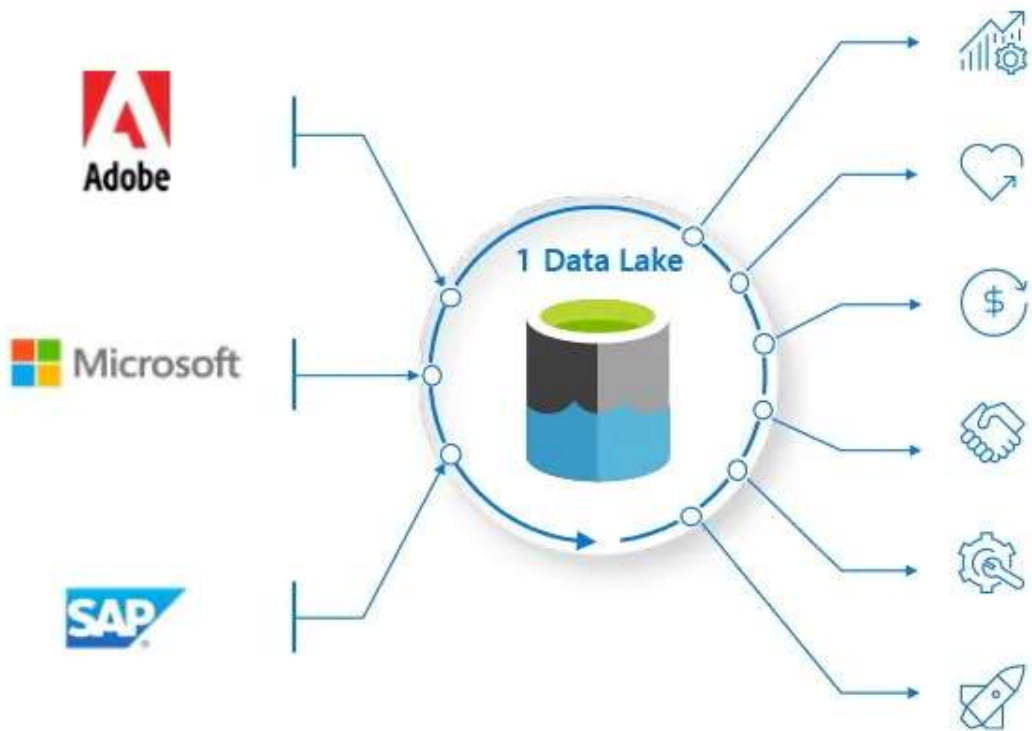
работники сервисов доставки еды и такси жалуются, что компании не сообщают, как именно алгоритмы их оценивают, а в случае ошибки работники не могут получить компенсацию. Сегодня в сети появилась петиция, требующая от таких компаний как Uber, Deliveroo, Bolt, Amazon Flex, Just Eat, Free Now, and Ola раскрыть принципы работы алгоритмов.

Uber управляет десятками тысяч водителей с помощью ИИ. Они занимаются всем: от распознавания лица для проверки личности до выявления мошенничества среди водителей.

Сервис доставки еды Deliveroo в своей политике конфиденциальности открыто заявляет, что ручные проверки «просто невозможны в те сроки и при тех объемах доставки, которыми мы занимаемся».

Существует пример лондонского водителя с отличным рейтингом, который в июле прошлого года получил от Uber предупреждение, что он замечен в мошеннических действиях. Две недели спустя водитель получил второе. После третьего аккаунт подлежит блокировке. После безуспешных попыток получить объяснения от компании, водитель обратился в профсоюз Workers Info Exchange (WIE). В итоге Uber признал ошибку и принёс извинения.

# 1132 Open Data Initiative от SAP, Adobe и Microsoft

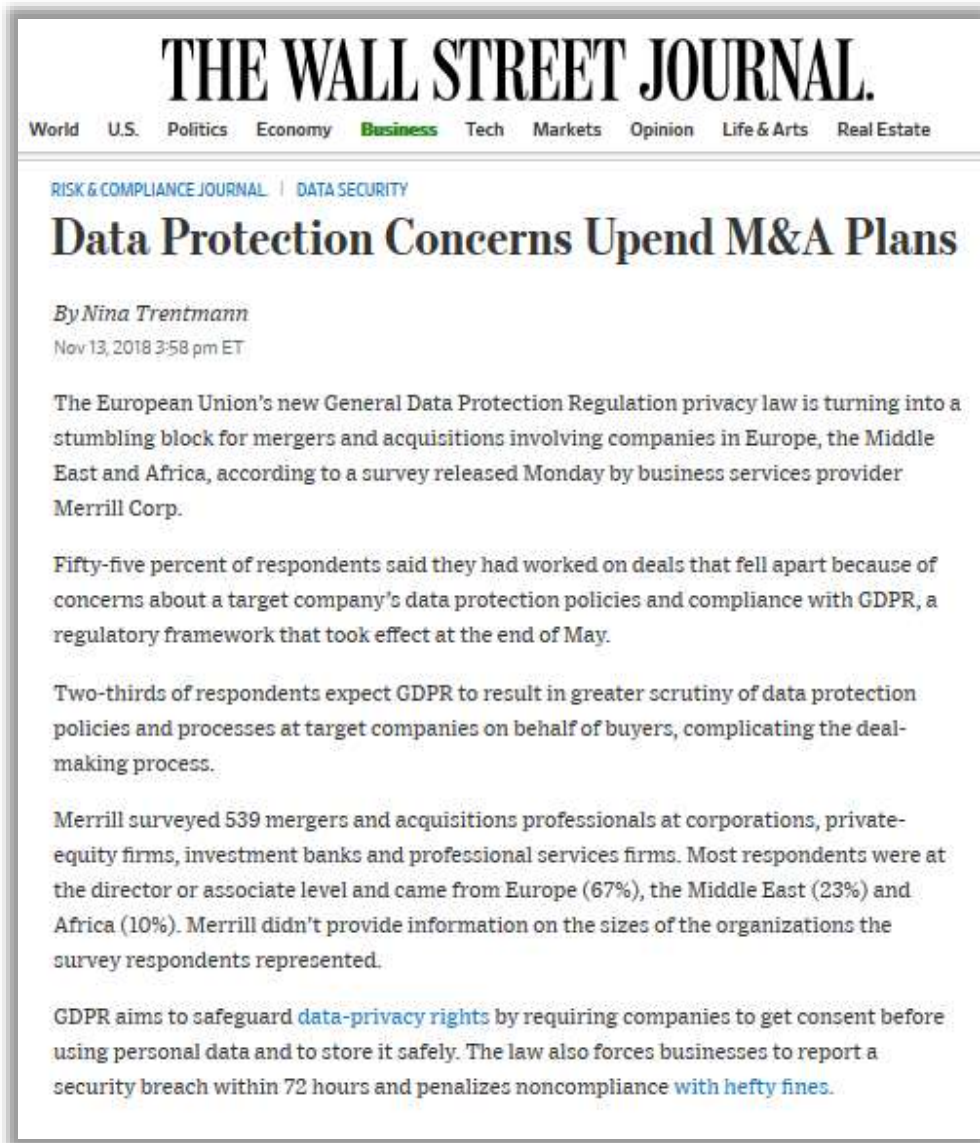


Производители программного обеспечения SAP и Adobe Systems, а также американская корпорация Microsoft заявили о создании альянса Open Data Initiative, призванного обеспечить эффективное использование всех данных о клиентах, собираемых разными приложениями через разные каналы (онлайновые и офлайновые), хранящихся в разных местах и контролируемых разными субъектами, а также позволить выполнить требования GDPR о переносимости персональных данных.

Со стороны бизнеса идею Open Data Initiative поддержали такие крупные компании, как Coca-Cola, Unilever и Walmart. Эксперты полагают, что ее успех будет во многом зависеть от того, присоединятся ли к альянсу такие лидеры рынка CRM, как Oracle и Salesforce.

<https://www.reuters.com/article/us-microsoft-sap-se-idUSKCN1M41L6>  
<https://www.microsoft.com/en-us/open-data-initiative>

## 1133 Негативное влияние GDPR на сделки по слиянию и поглощению



**THE WALL STREET JOURNAL.**

World U.S. Politics Economy **Business** Tech Markets Opinion Life & Arts Real Estate

RISK & COMPLIANCE JOURNAL | DATA SECURITY

### Data Protection Concerns Upend M&A Plans

By *Nina Trentmann*  
Nov 13, 2018 3:58 pm ET

The European Union's new General Data Protection Regulation privacy law is turning into a stumbling block for mergers and acquisitions involving companies in Europe, the Middle East and Africa, according to a survey released Monday by business services provider Merrill Corp.

Fifty-five percent of respondents said they had worked on deals that fell apart because of concerns about a target company's data protection policies and compliance with GDPR, a regulatory framework that took effect at the end of May.

Two-thirds of respondents expect GDPR to result in greater scrutiny of data protection policies and processes at target companies on behalf of buyers, complicating the deal-making process.

Merrill surveyed 539 mergers and acquisitions professionals at corporations, private-equity firms, investment banks and professional services firms. Most respondents were at the director or associate level and came from Europe (67%), the Middle East (23%) and Africa (10%). Merrill didn't provide information on the sizes of the organizations the survey respondents represented.

GDPR aims to safeguard [data-privacy rights](#) by requiring companies to get consent before using personal data and to store it safely. The law also forces businesses to report a security breach within 72 hours and penalizes noncompliance [with hefty fines](#).

Согласно опросу, опубликованному в ноябре 2018 г. провайдером бизнес-услуг Merrill Corp., GDPR становится камнем преткновения для слияний и поглощений с участием компаний в Европе, на Ближнем Востоке и в Африке.

Пятьдесят пять процентов респондентов заявили, что работали над сделками, которые развалились из-за опасений относительно состояния защиты данных в целевых компаниях и их соответствия требованиям GDPR.

Две трети респондентов ожидают, что потенциальные компании-покупатели будут более тщательно подходить к проверке политик и процедур защиты персональных данных в целевых компаниях, что усложнит процесс заключения сделок.

## 1134 Google – крупнейший бенефициар?

### Study: Google is the biggest beneficiary of the GDPR

Thanks to its dominant market position, the industry leader benefits from a stronger concentration in the online advertising market. Although the number of trackers is decreasing overall, a few large tracking operators such as Google receive even more user data.



10/10/2018



Thom Cref  
Editor

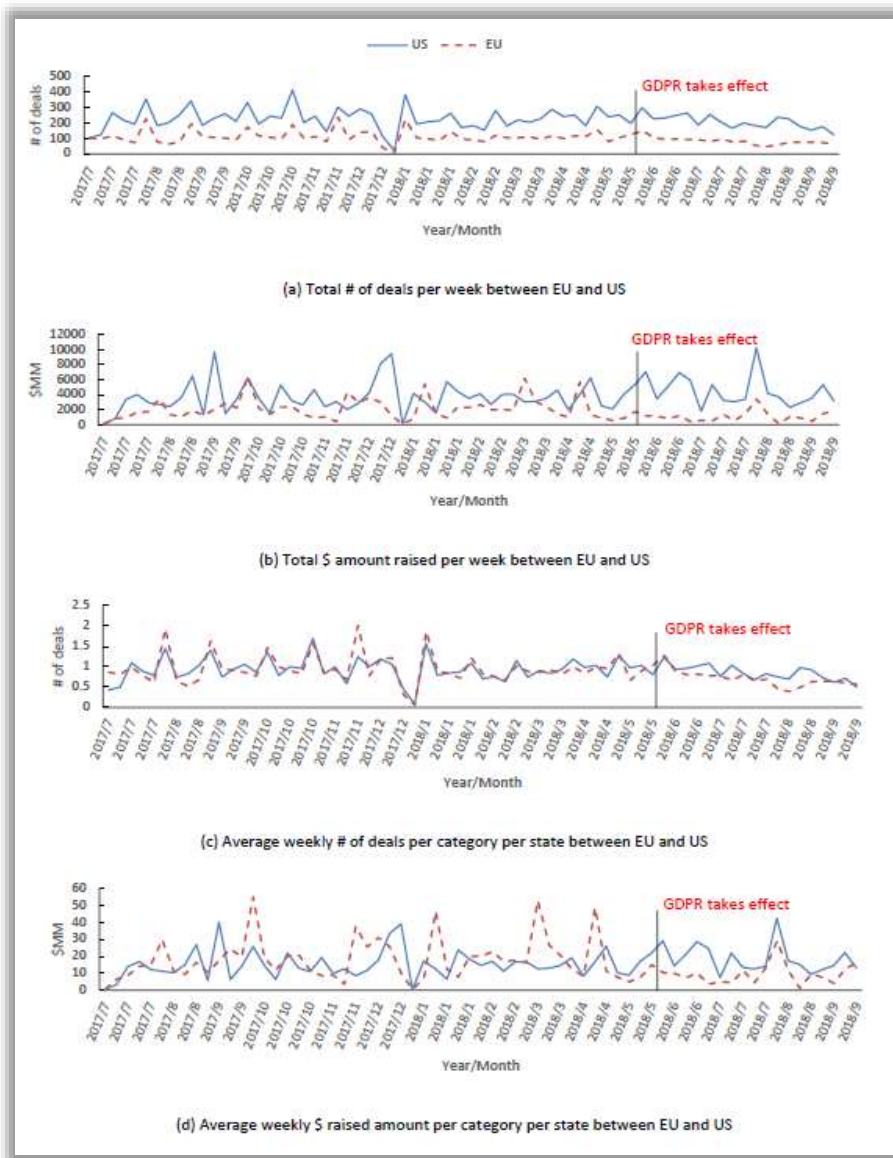
[Blog](#)

The General Data Protection Regulation (GDPR), which primarily aims to protect personal data within the EU, has been in effect for a little over four months now. But what has changed since 25th of May? What impact did the GDPR have on the tracker landscape and the online advertising market in Europe? A study by Cliqz and Ghostery answers these questions. Using data from [WhoTracks.me](#), it compares the prevalence of trackers one month before and one month after the introduction of the GDPR.

[WhoTracks.me](#) is a joint initiative of Cliqz and Ghostery. It provides structured information on tracking technologies, market structure and data-sharing on the web and thus creates more transparency. On the [WhoTracks.me](#) website, interested parties will find visualized monthly tracker statistics. They are based on the evaluation of around 300 million-page loads and more than half a million websites.

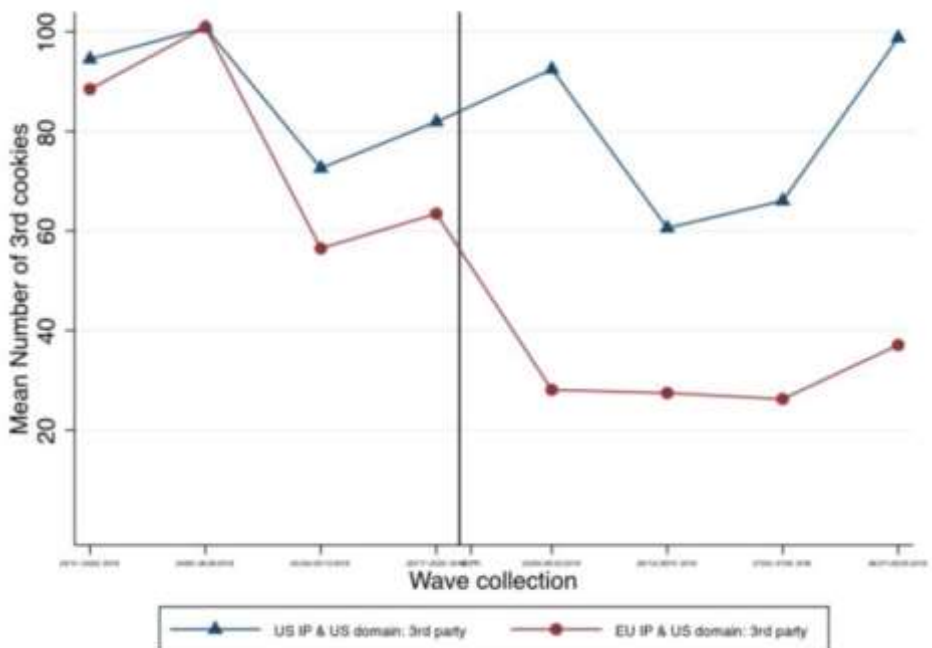
Согласно выводам исследования Ghostery and Cliqz, благодаря своей доминирующей позиции на рынке, лидер отрасли выигрывает от более сильной концентрации на рынке онлайн-рекламы. Хотя количество (программ, отслеживающих действия посетителей и пользователей вебсайтов) на рынке в целом снижается, несколько крупных компаний-контролеров, таких как Google, получают еще больше пользовательских данных.

## Краткосрочное влияние GDPR на венчурные инвестиции в информационные технологии



Согласно выводам исследования National Bureau of Economic Research, GDPR оказал негативное влияние на европейские стартапы по сравнению их американскими коллегами. Например, общий объем венчурного капитала, инвестированного в стартапы ЕС, упал на 50% из-за внедрения GDPR. Кроме того, на 17,6% сократилось количество еженедельных венчурных сделок и на 39,6% уменьшилось количество привлеченных средств в среднем на каждую сделку.

# 1136 Влияние GDPR на контент-провайдеров, существующих за счет рекламы



Number 3<sup>rd</sup> Party Cookies – US Sites

Согласно выводам исследования University of Paris Sud, Carnegie Mellon University и University of Minnesota, влияние GDPR привело к:

- уменьшению количества сторонних файлов cookie и запросов на сайтах;
- наличию некоторых ограничений над доступ к сайтам с европейских IP-адресов, включая около 20% американских новостных и медиа сайтов имеют ограничения по доступу для посетителей ЕС;
- малое влияние на количество и качество посещений сайтов, а на европейских сайтах наблюдается увеличение количества посещений по сравнению с сайтами США.



[https://www.ftc.gov/system/files/documents/public\\_events/1415032/privacycon2019\\_cheyre\\_impact\\_gdpr\\_on\\_ad-supported\\_content\\_providers.pdf](https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_cheyre_impact_gdpr_on_ad-supported_content_providers.pdf)



## Вступление в силу GDPR в Европе совпало с резким падением числа приложений для Android



The Register

### Europe's GDPR coincides with dramatic drop in Android apps

Privacy rules increase cost, reduce choice, slash revenues, study concludes

Thomas Claburn Mon 9 May 2022 23:00 UTC

Europe's data protection regime has reduced the number of apps available in Google Play by "a third," increased costs, and reduced developer revenues, according to a study published Monday.

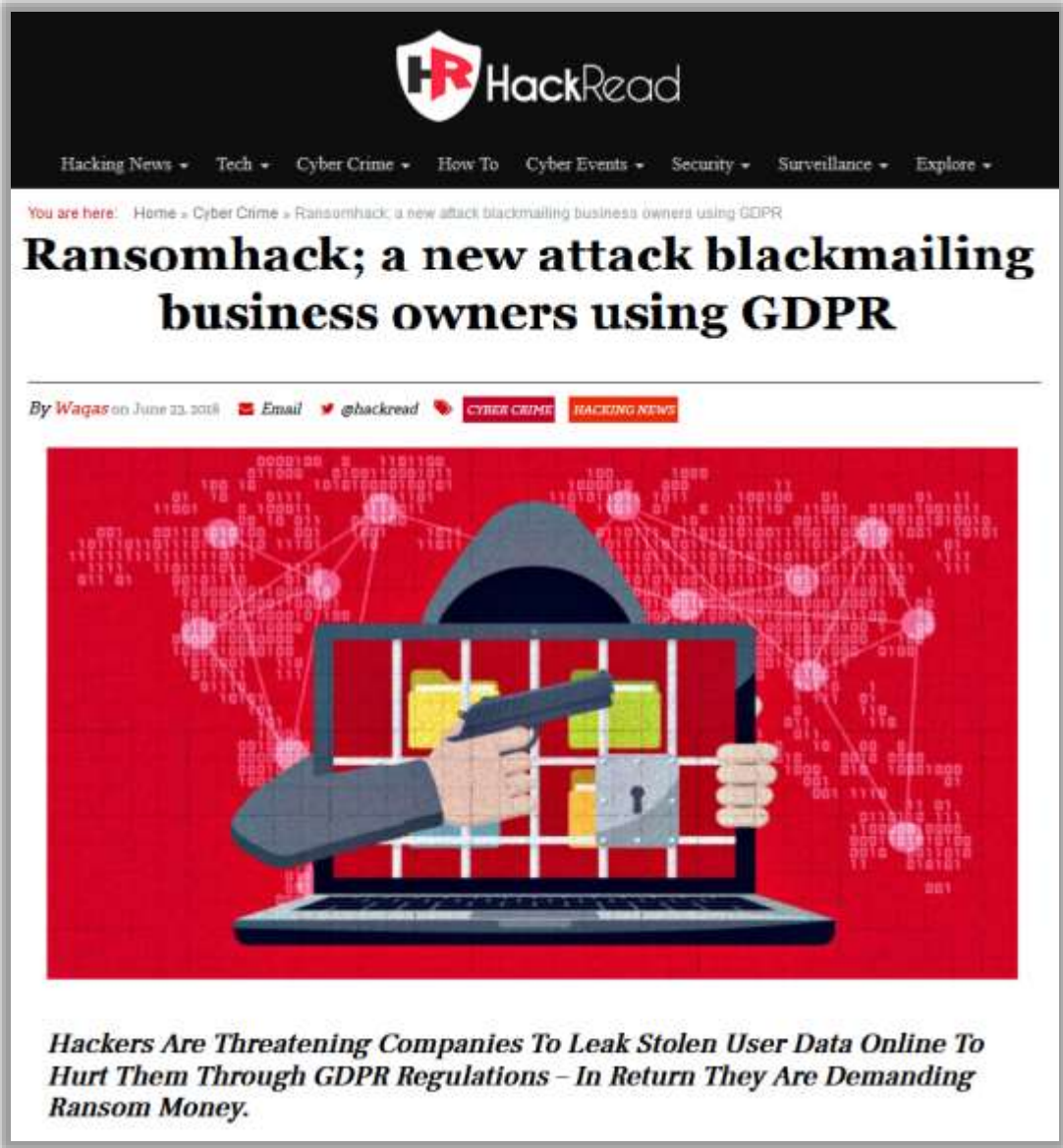
And with higher costs, fewer apps are being created, to the detriment of consumers and the mobile app economy, it claims.

"At the start of our sample period in July 2016, our data on the contain 2.1 million apps in the Google Play Store, while AppBrain reported 2.2 million.<sup>26</sup> The number of Play Store apps in our sample then rises to 2.8 million in the fourth quarter of 2017, then falls by almost one million – about 32 percent – by the end of 2018. Available apps in AppBrain saw a similar decline, by 31 percent between the beginning of 2018 and the end of 2018

In a paper titled, "GDPR and the Lost Generation of Innovative Apps", economic researchers Rebecca Janßen (ZEW Mannheim, Germany), Reinhold Kesler (University of Zurich, Switzerland), Michael Kummer (University of East Anglia, UK) & Joel Waldfogel (University of Minnesota, USA) examined the impact of Europe's General Data Protection Regulation (GDPR) on the mobile app business.

Европейский режим защиты данных сократил количество приложений, доступных в Google Play, на треть, увеличил расходы и снизил доходы разработчиков, говорится в исследовании,. А в результате увеличения расходов создается меньше приложений, что наносит ущерб потребителям и экономике мобильных приложений.

Исследователи изучили 4,1 миллиона приложений, доступных через Google Play в период с июля 2016 года по октябрь 2019 года. В настоящее время в Google Play доступно около 3,48 млн приложений, по сравнению с примерно 2,2 млн в 2016 году.



The image shows a screenshot of a news article from HackRead. At the top, the HackRead logo is visible, followed by a navigation menu with categories like 'Hacking News', 'Tech', 'Cyber Crime', 'How To', 'Cyber Events', 'Security', 'Surveillance', and 'Explore'. Below the navigation, the breadcrumb trail reads 'You are here: Home > Cyber Crime > Ransomhack; a new attack blackmailing business owners using GDPR'. The main title of the article is 'Ransomhack; a new attack blackmailing business owners using GDPR'. Below the title, it says 'By Waqas on June 23, 2018' and includes social media icons for Email, @hackread, CYBER CRIME, and HACKING NEWS. The central image is a red-themed illustration of a person in a hoodie holding a handgun, with a laptop in front of them. The laptop screen shows a padlock and a key, symbolizing ransomware or data theft. The background features binary code and network connections. Below the illustration, there is a summary text: 'Hackers Are Threatening Companies To Leak Stolen User Data Online To Hurt Them Through GDPR Regulations - In Return They Are Demanding Ransom Money.'

**Авторы мошеннической  
схемы ransomhack используют  
GDPR для шантажа компаний  
и получения выкупа**

Взломав серверы очередной жертвы и похитив персональную информацию, преступники не планируют её как-либо использовать, а лишь угрожают публикацией. В соответствии с GDPR компанию ждет крупный штраф в случае утечки, поэтому, чтобы не попасть под санкции Европейского Союза, организации предпочитают выполнить требования злоумышленников.

## Хакер получил доступ к 400 млн аккаунтов Twitter и предлагает Илону Маску выкупить их

A threat actor is claiming they have obtained data of 400,000,000 Twitter users and is offering it for sale.

A threat actor claims they have obtained data of 400,000,000 Twitter users and is attempting to sell it.

The seller claims the database is private, he provided a sample of 1,000 accounts as proof of claims which included the private information of prominent users such as Donald Trump JR, Brian Krebs, and many more:

The seller, a member of data breach forums named Ryushi, claims the data was scraped via a vulnerability, it includes emails and phone numbers of celebrities, politicians, companies, normal users, and a lot of OG and special usernames.

The seller is also inviting Twitter and Elon Musk to buy the data to avoid GDPR lawsuits.

*"Twitter or Elon Musk if you are reading this you are already risking a GDPR fine over 5.4m breach imaging the fine of 400m users breach source. Your best option to avoid paying \$276 million USD in GDPR breach fines like facebook did (due to 533m users being scraped) is to buy this data exclusively." reads the advertising.*

The seller also announced that the sale is covered by the escrow service offered by the Breached forum administrators (pompompurin).

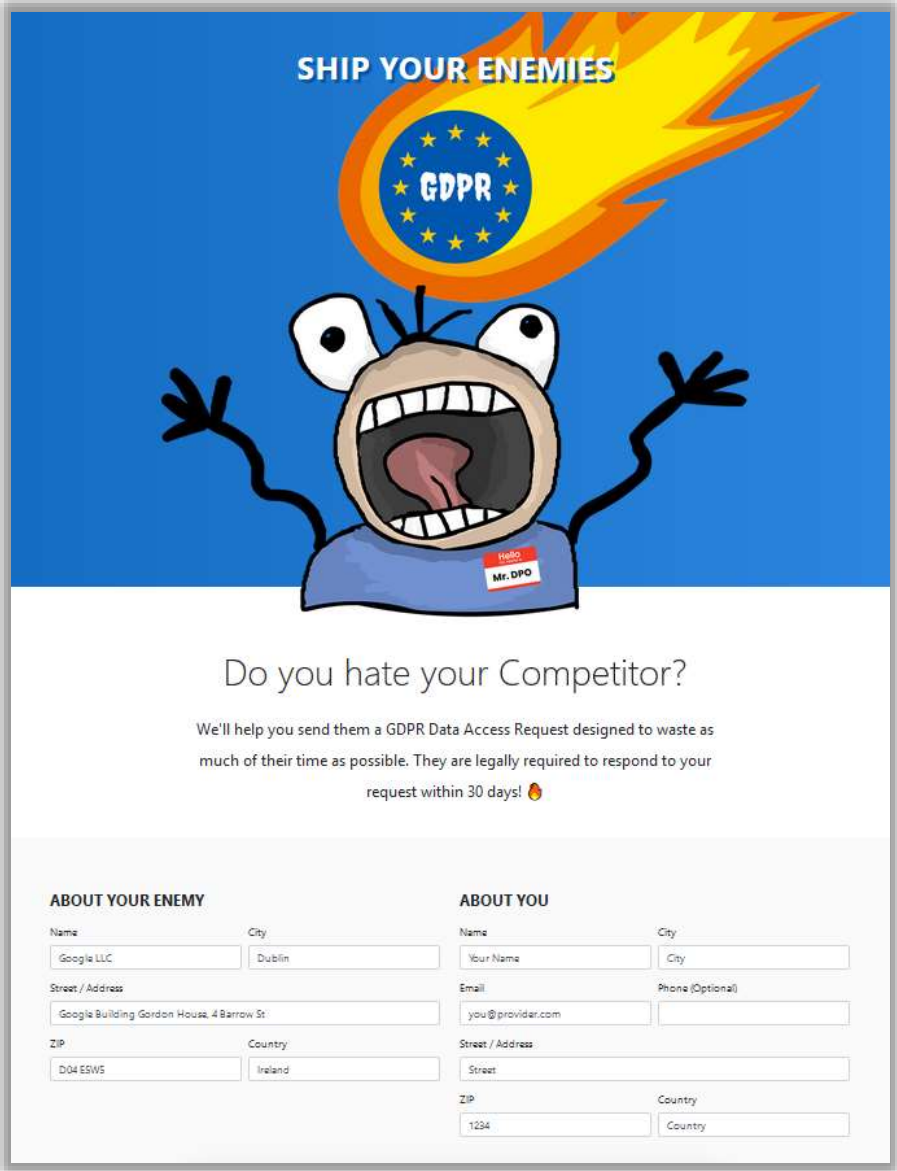
Неизвестный хакер утверждает, что получил доступ к 400 млн учетных записей пользователей Twitter. По его словам, выкупить их должен никто иной, как глава компании Илон Маск.

«Twitter или Илон Маск, если вы читаете это, вы уже рискуете получить штраф GDPR [общий регламент по защите персданных, действующий в ЕС — прим. ред.] за утечку 5,4 млн аккаунтов. Представьте себе штраф за 400 млн слитых учетных записей. Ваш лучший вариант избежать штрафа в размере \$276 млн за нарушение GDPR, как это сделал Facebook (за слив 533 млн пользователей), — это купить эти данные на эксклюзивной основе», — заявил хакер.

<https://www.gazeta.ru/tech/news/2022/12/26/19358137.shtml>

<https://securityaffairs.co/wordpress/139993/data-breach/twitter-400-million-users-leak.html>

# 1140 Создание административной нагрузки посредством GDPR



**SHIP YOUR ENEMIES**

Do you hate your Competitor?

We'll help you send them a GDPR Data Access Request designed to waste as much of their time as possible. They are legally required to respond to your request within 30 days! 🍌

**ABOUT YOUR ENEMY**

Name	City
Google LLC	Dublin
Street / Address	
Google Building Gordon House, 4 Barrow St.	
ZIP	Country
D04 E9W5	Ireland

**ABOUT YOU**

Name	City
Your Name	City
Email	Phone (Optional)
you@provider.com	
Street / Address	
Street	
ZIP	Country
1234	Country

## Web-сервис «Ship your enemies»

Автор сайта (Jerre Baum) предлагает всем желающим воспользоваться бесплатным сервисом и направлять от своего имени запросы на доступ к персональным данным, реализуя право согласно ст.15 GDPR.

При этом публично заявляться не позитивная цель в виде защиты прав и законных интересов субъектов персональных данных, а возможность «усложнить жизнь» адресатам такого запроса. Также автор преследует цель продемонстрировать несовершенство и «глупость» некоторых положений GDPR.

## Weaponizing the GDPR

boingboing / CORY DOCTOROW / 6:20 PM TUE OCT 8, 2019

### Gamers propose punishing Blizzard for its anti-Hong Kong partisanship by flooding it with GDPR requests



Being a global multinational sure is hard! Yesterday, World of Warcraft maker Blizzard faced [global criticism](#) after it disqualified a high-stakes tournament winner over his statement of solidarity with the [Hong Kong protests](#) -- Blizzard depends on mainland China for a massive share of its revenue and it can't afford to offend the Chinese state.

Today, outraged games on Reddit's [/r/hearthstone](#) forum are [scheming](#) a plan to flood Blizzard with punishing, expensive personal information requests under the EU's expansive [General Data Privacy Regulation](#) -- Blizzard depends on the EU for another massive share of its revenue and it can't afford the enormous fines it would face if it failed to comply with these requests, which take a lot of money and resource to fulfill.

В октябре 2019 года компания Blizzard (издатель игры World of Warcraft) подверглась широкой критике от игроков после дисквалификации победителя игрового турнира за его заявление о солидарности с протестами в Гонконге.

Значительное количество фанатов игры посредством координации своих действий на форуме Reddit / r / hearthstone планируют максимально осложнить жизнь Blizzard путем реализации своих прав на доступ к информации как субъектов персональных данных, предоставленных им положениями ст. 15 GDPR – «Right of access by the data subject».

## Microsoft прислушалось к позиции EDPS в отношении своей роли в качестве контролера

### EDPS investigation into IT contracts: stronger cooperation to better protect rights of all individuals

21  
Oct  
2019

EDPS investigation into IT contracts: stronger cooperation to better protect rights of all individuals

Press Release

Cooperation between public authorities in the Member States, EU institutions and other international organisations is essential to ensure that **contractual arrangements and measures with Microsoft provide the same level of protection for individual rights throughout the European Economic Area (EEA)**. Amended contractual terms, technical safeguards and settings agreed between the Dutch Ministry of Justice and Security and Microsoft to **better protect the rights of individuals** shows that there is significant scope for improvement in the development of contracts between public administration and the most powerful software developers and online service outsourcers. The EDPS is of the opinion that such solutions should be extended not only to all public and private bodies in the EU, which is our short-term expectation, but also to individuals, the Assistant EDPS said today.

In April 2019, the European Data Protection Supervisor (EDPS) **launched an investigation** into the use of Microsoft products and services by EU institutions. The investigation identified the Microsoft products and services used by the EU institutions and assessed whether the contractual agreements concluded between Microsoft and the EU institutions are fully compliant with data protection rules. The EDPS also considered whether there were appropriate measures in place to mitigate risks to the data protection rights of individuals when EU institutions use Microsoft products and services.

Европейский инспектор по защите данных (EDPS) от 21 октября 2019 года опубликовал отчет, в котором высказаны серьезные опасения по поводу соблюдения компанией Microsoft требований GDPR и роль Microsoft как процессора данных для публичных органов и организаций ЕС. В этом отчете отмечается, что существует значительный потенциал для улучшения разработки контрактов между публичными органами и самыми влиятельными разработчиками программного обеспечения и аутсорсерами онлайн-услуг.

Это произошло на фоне споров о том, кто контролирует данные, когда определенные сервисы и ПО Microsoft обслуживают европейские организации, а затем «сообщают домой» данные об использовании этих сервисов и ПО.

В ноябре 2019 года Компания Microsoft обновила свои Online Services Terms (OST) и теперь признает свою роль как контролера данных при GDPR при предоставлении облачных сервисов и использовании ПО. Изменения прорабатывались совместно с the Министерством юстиции и безопасности Нидерландов (Dutch Ministry of Justice and Security).

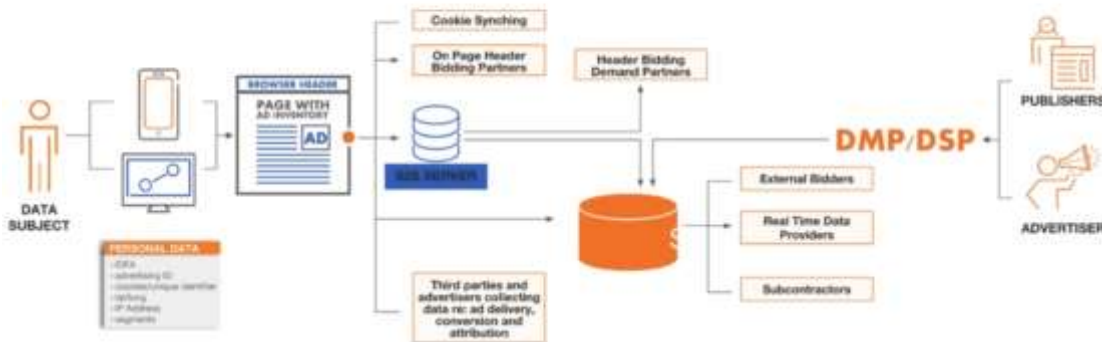
## Пользователи Google в Великобритании могут быть выведены из-под действия GDPR



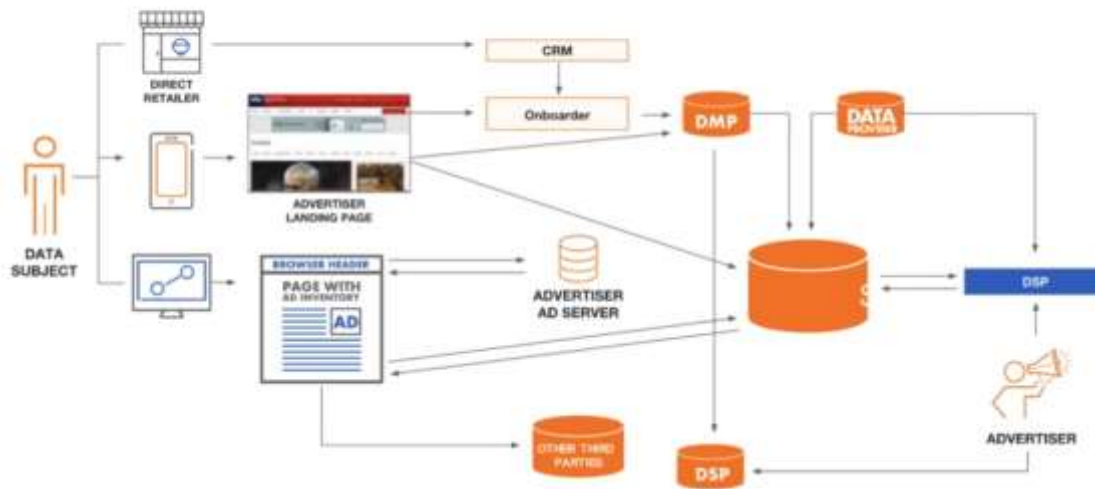
По сообщению источников Reuters, Google планирует вывести в юрисдикцию США учетные записи своих британских пользователей из-под контроля надзорных органов Европейского Союза. Такая возможность появилась благодаря Brexit. Google намерен потребовать от своих британских пользователей принятия ими новых условий обслуживания, включая применение американской юрисдикции.

## Спор Google и европейских компаний о согласиях на онлайн рекламу и составление цифрового профиля

### AdTech Data Flows... Sell-side



### AdTech Data Flows... Buy-side



Согласно требованиям Transparency and Consent Framework консорциума IAB Europe, участниками которого являются большинство ведущих игроков рынка онлайн рекламы, чтобы сайты могли зарабатывать на рекламе, пользователи должны дать два отдельных согласия — на показ персонализированной рекламы и на то, что данные пользователя будут собираться в его рекламный профиль и анализироваться.

Некоторые сайты и медиаплатформы хотят убрать вторую опцию. Но тогда Google не сможет анализировать поведение пользователей, чтобы показывать им таргетированную рекламу. Поэтому Google требует, чтобы сайты, зарабатывающие на Google Ads, вынуждали пользователей давать оба согласия.



# 1145 Meta допустила возможность закрытия Facebook и Instagram в Европе

The image shows the cover page of a Form 10-K filed with the United States Securities and Exchange Commission. The form is for Meta Platforms, Inc., a Delaware corporation, for the year ended December 31, 2021. The company's principal executive office is located at 1001 Willow Road, Menlo Park, California 94025. The form is filed with the SEC under Commission File Number 001-25551. The document includes the company's logo and name, and lists the registrant's address and contact information. It also includes a table of securities registered pursuant to Section 12(b) of the Act, showing Class A Common Stock with a par value of \$0.00001 per share, trading on the Nasdaq Stock Market LLC. The form is a 28-page document.

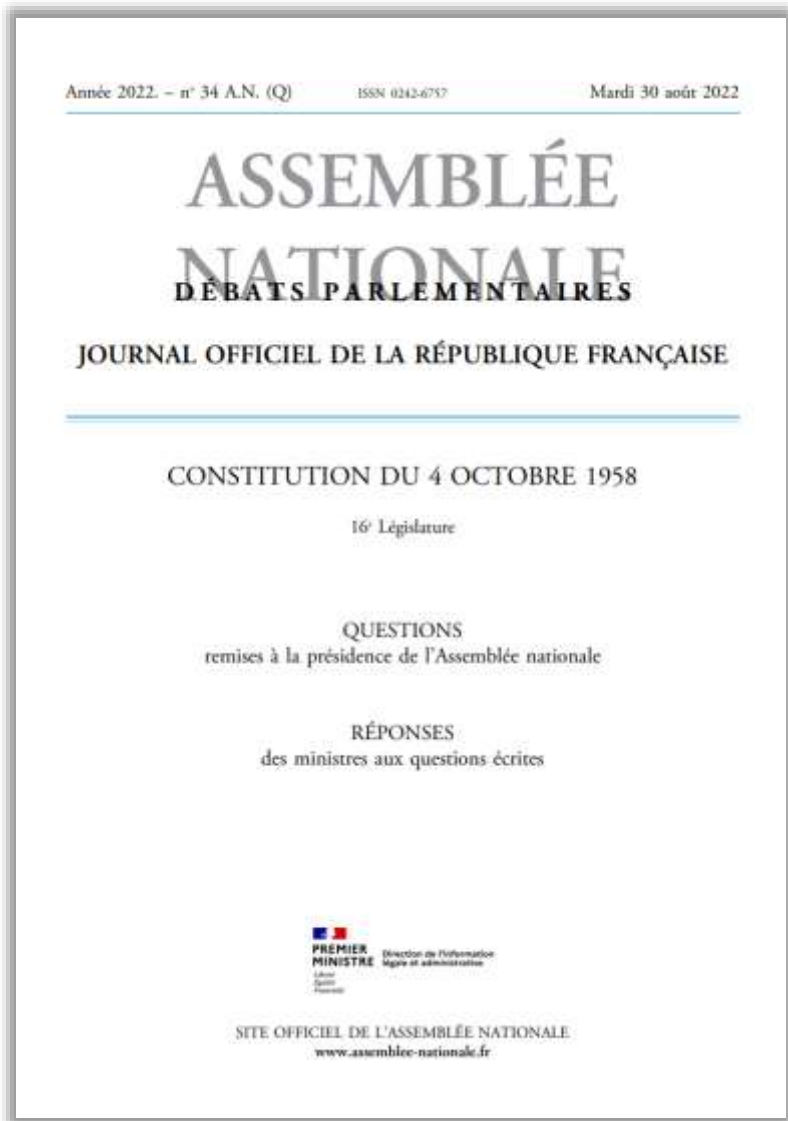
Корпорация Meta рассматривает возможность отключения соцсетей Facebook и Instagram в Европе. Решение связано с законом Евросоюза, согласно которому данные европейских пользователей должны храниться и обрабатываться на европейских серверах (сейчас данные находятся еще и в США). Об этом сообщается в годовом отчете для Комиссии по ценным бумагам и биржам США.

Meta использует трансатлантические структуры передачи данных: Privacy Shield (признана недействительной Евросоюзом в июле 2020 года из-за нарушений защиты данных) и SCC (стандартные положения о защите данных). «Обмен данными между странами и регионами имеет решающее значение для предоставления своих услуг и целевой рекламы», — сказано в отчете.

«Отсутствие безопасной, надежной и законной международной передачи данных нанесет ущерб экономике и помешает росту бизнеса, основанного на данных, в ЕС, в то время как мы пытаемся восстановиться после COVID-19», — заявил вице-президент корпорации по глобальным вопросам и коммуникациям Ник Клегг.

Также господин Клегг призвал «регулирующие органы применять пропорциональный и прагматичный подход, чтобы минимизировать перебои в работе многих тысяч компаний».

## 1146 Франция запретила Microsoft Office 365 и Google Workspace в школах



Министр национального образования и молодёжи Франции Пап Ндьей (Pap Ndiaye) заявил о том, что бесплатные версии Microsoft Office 365 и Google Workspace не должны использоваться школами. Официально позиция министра объясняется тем, что, согласно закону, французские госконтракты на поставку требуют оплаты. Бесплатные услуги в принципе не рассматриваются при закупках.

По данным techzine.eu, реальная причина состоит в том, что продукты не соответствуют нормам GDPR, закона ЕС о защите персональных данных (ПД), и решению европейского суда, который в июле 2020 назвал незаконным механизм передачи ПД из Европы в США, использовавшийся тысячами компаний, известный также как «Щит конфиденциальности» (Privacy Shield).

Французские власти ещё в 2021 году опубликовали указание не хранить данные посредством облачных сервисов Microsoft 365 для недопущения возможных взломов и использования [данных] американской разведкой.

## 1147 Еврокомиссия заявила, что WhatsApp согласился выполнять правила ЕС

WhatsApp обязался соблюдать правила Евросоюза и быть более прозрачным в отношении изменений условий обслуживания пользователей. Об этом сообщила в понедельник пресс-служба Еврокомиссии (ЕК).

"После диалога с органами ЕС по защите прав потребителей и Еврокомиссией сеть WhatsApp обязался быть более прозрачной в отношении изменений своих условий обслуживания. Более того, компания упростит пользователям отказ от обновлений, если они с ними не согласны, и четко объяснит, когда такой отказ приводит к тому, что пользователь больше не может пользоваться услугами WhatsApp", - отмечается в заявлении ЕК.

Кроме того, как подчеркивается в документе, "WhatsApp подтвердил, что личные данные пользователей не передаются третьим лицам или другим компаниям Meta, включая Facebook, в рекламных целях".

"Для любых будущих обновлений политики WhatsApp будет объяснять, какие изменения намерен внести в договоры пользователей и как они могут повлиять на их права; включать возможность отклонить обновленные условия обслуживания так же заметно, как и возможность их принять; гарантировать, что уведомления, информирующие об обновлениях, могут быть отклонены или просмотр обновлений может быть отложен, а также уважать выбор пользователей и воздерживаться от отправки повторных уведомлений", - добавила ЕК.

ЕК напоминает, что в январе 2022 года Брюссель отправил письмо руководству мессенджера относительно "предполагаемых недобросовестных действий в контексте обновлений WhatsApp условий обслуживания и политики конфиденциальности". В июне тогда же года ЕК отправила повторное письмо с просьбой "четко информировать пользователей о бизнес-модели WhatsApp и, в частности, о том, получает ли WhatsApp доход от коммерческой политики, касающейся личных данных пользователей".

# 1148 Threads недоступен в Европе даже через VPN

## Meta confirms it is blocking EU-based users from accessing Threads via VPN

Ivan Mehta · gendiarotk / 2:29 PM GMT+3 · July 14, 2023 Comment




Image Credits: DeFodi Images / Contributor / Getty Images

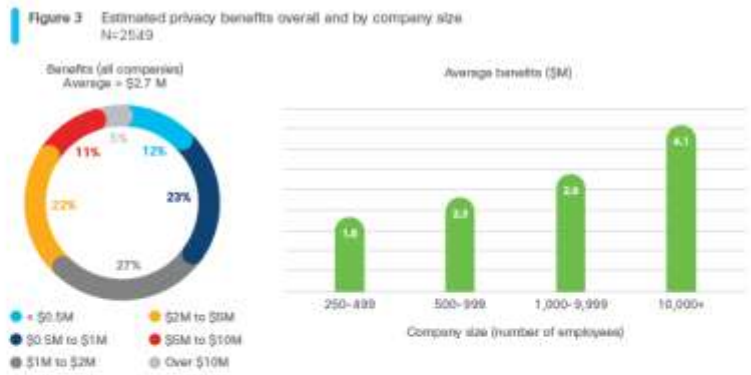
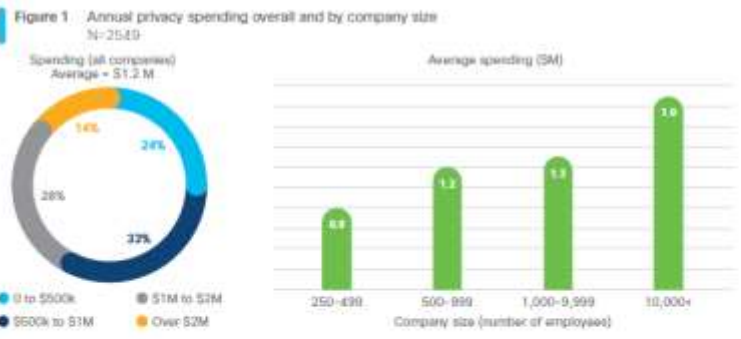
After multiple EU-based users complained about not being able to access [Instagram's Threads app](#) through VPN, Meta confirmed that it is blocking such efforts.

The company launched Threads last week, but given privacy concerns around the app, [it is not available in the EU](#). The company said in a statement that it has applied further measures to stop users from accessing the new social app.

"Threads is not currently available in most countries in Europe and we've taken additional steps to prevent people based there from accessing it at this time. Europe continues to be an incredibly important market for Meta and we hope to make Threads available here in the future," it said in a statement provided to TechCrunch.

Доступ европейцам к соцсети Threads (аналог Twitter) невозможен даже при помощи VPN-сервисов. Соцсеть была запущена в начале июля, но она недоступна для европейцев – для работы в ЕС Meta сначала должна отрегулировать вопрос обмена данными между новой платформой и Instagram. «Европа по-прежнему остаётся очень важным рынком для Meta, и мы надеемся сделать Threads доступными здесь в будущем», — говорится в заявлении компании изданию.

# От конфиденциальности к прибыли: достижение положительного дохода от инвестиций в приватность



**Figure 5 Average privacy returns by country**  
Global average: Benefits = 2.7 times investment  
N=2543



**Figure 2 Business impact of privacy**  
Percentage of companies getting significant benefits in each area, N=2549



**Figure 4 Distributions of privacy returns, percent of respondents**  
N=2543



Исследование Cisco за 2019 год «From Privacy to Profit: Achieving Positive Returns on Privacy Investments», согласно которому на каждый 1 доллар, потраченный организацией на Privacy, они получают возврат инвестиций в размере 2,70 доллара.

1150 Сравнительное исследование Data Privacy за 2022г. от Cisco

Privacy Investment Brings Attractive Returns

Ratio of Privacy Benefits to Investment

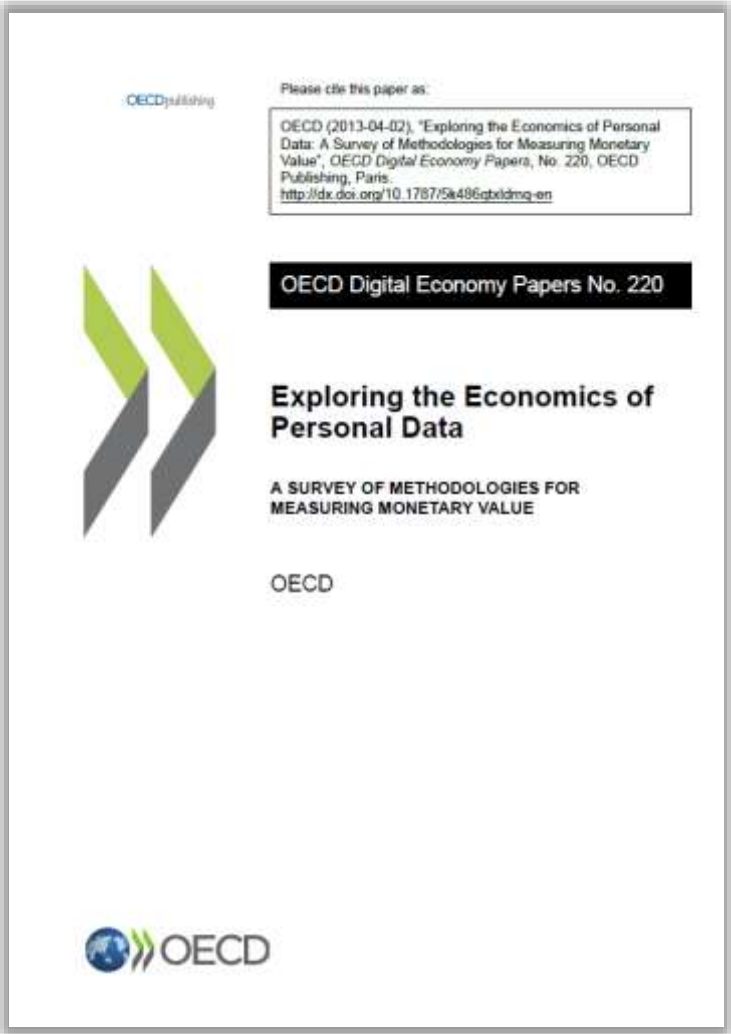


Privacy-Mature Organizations Achieve Higher ROI

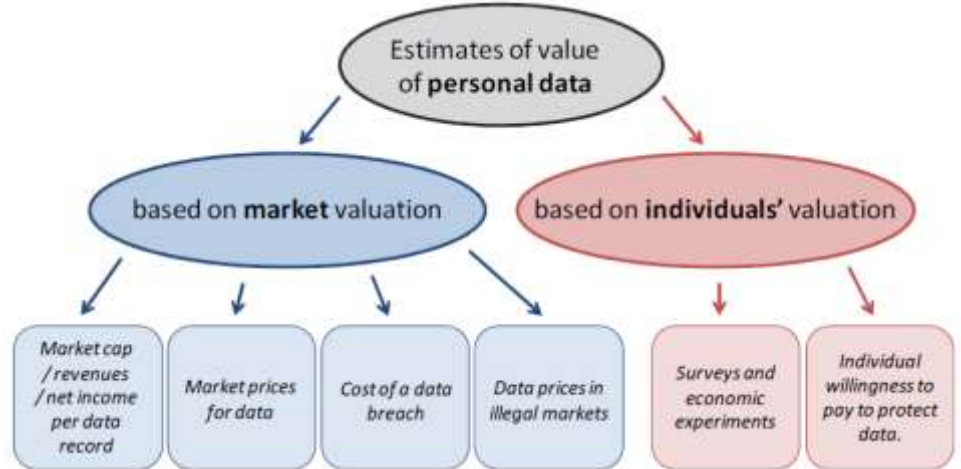


Privacy Laws Seen Positively Around the World





Personal data	Collection / access	Storage and aggregation	Analysis and distribution	Usage
<b>Volunteered</b> e.g. declared hobbies and interests, preferences, expertise, etc.	<ul style="list-style-type: none"> <li>• Mobile phones</li> <li>• Blogs and discussion lists</li> <li>• Social, professional and special interest networks</li> </ul>	<ul style="list-style-type: none"> <li>• ISPs and phone providers</li> <li>• Government agencies (e.g. tax offices, property registries, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>• Retailers and service providers</li> <li>• Public administration</li> <li>• Financial institutions</li> </ul>	<ul style="list-style-type: none"> <li>• Businesses</li> <li>• Government and public sector agencies</li> <li>• End users.</li> </ul>
<b>Observed</b> e.g. location information, browser history, shopping habits etc.	<ul style="list-style-type: none"> <li>• User-generated content</li> <li>• Loyalty schemes operated by retailers</li> </ul>	<ul style="list-style-type: none"> <li>• On-line social networks,</li> <li>• Financial institutions</li> <li>• Medical practitioners</li> </ul>	<ul style="list-style-type: none"> <li>• Healthcare providers</li> <li>• Specialized companies involved in online advertising and market research,</li> </ul>	
<b>Inferred</b> e.g. credit ratings, profiles built from online activities, etc.	<ul style="list-style-type: none"> <li>• Smart appliances</li> <li>• Applications</li> <li>• Sensors</li> <li>etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Utility service providers</li> <li>• Retailers</li> <li>etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Data analysts, providers and brokers</li> <li>etc.</li> </ul>	



## The Economics of Privacy<sup>1</sup>

ALESSANDRO ACQUISTI, CURTIS TAYLOR, AND LIAD WAGMAN\*

*This article summarizes and draws connections among diverse streams of theoretical and empirical research on the economics of privacy. We focus on the economic value and consequences of protecting and disclosing personal information, and on consumers' understanding and decisions regarding the trade-offs associated with the privacy and the sharing of personal data. We highlight how the economic analysis of privacy evolved over time, as advancements in information technology raised increasingly nuanced and complex issues. We find and highlight three themes that connect diverse insights from the literature. First, characterizing a single unifying economic theory of privacy is hard, because privacy issues of economic relevance arise in widely diverse contexts. Second, there are theoretical and empirical situations where the protection of privacy can both enhance and detract from individual and societal welfare. Third, in digital economies, consumers' ability to make informed decisions about their privacy is severely hindered because consumers are often in a position of imperfect or asymmetric information regarding when their data is collected, for what purposes, and with what consequences. We conclude the article by highlighting some of the ongoing issues in the privacy debate of interest to economists. (JEL D82, D83, G20, I10, L13, M31, M37)*

### 1. Why an Economics of Privacy

The value and regulation of information assets have been among the most interesting areas of economic research since

Friedrich Hayek's 1945 treatise on the use of knowledge in society. Contributions to what has become known as the field of information economics have been among the most influential, insightful, and intriguing in the

\*Acquisti: Hertz College, Carnegie Mellon University; Taylor: Department of Economics, Duke University; Wagman: Stern School of Business, Yeshiva University of Technology. We are grateful for useful comments and suggestions provided by the reviewing team, as well as by Drew Bos-Sharot, Haimot Biderman, Alessandro Bonatti, Ryan Cahn, James Cooper, Ari Goldfarb, Jeroen Koopman, Clem Beudorck, Kai-Ling Hui, Nicole Justich, Joo-Hyeok Kim, Brad Malkin, Helen Nissenbaum, Andrew Odlyzko, Randall Peffer, Juan Png, Steven Postrel, Giancarlo Spagnolo, Lutz Straßmann, Catherine Tucker, Giovanni Valtieri.

Hal Varian, and Fredrick Zaidman Bergman. Acquisti gratefully acknowledges support from the Alfred P. Sloan Foundation and the Carnegie Corporation of New York via an Andrew Carnegie Fellowship. Taylor's research was supported in part by NSF grant SES-1132107. Wagman gratefully acknowledges support from the Yahoo Faculty Research and Engagement Program. The statements made and views expressed in this manuscript are solely the responsibility of the authors. All errors are the authors' own.  
<sup>1</sup>Go to <http://dx.doi.org/10.1257/jel.54.2.442> to visit the article page and view author disclosure statements.

В статье обобщаются и устанавливаются связи между различными потоками теоретических и эмпирических исследований в области экономики приватности. Авторы сосредоточились на экономической ценности и последствиях защиты и раскрытия личной информации, а также на понимании и решениях потребителей относительно компромиссов, связанных с конфиденциальностью и совместным использованием личных данных.

Авторы обнаружили и выделили три темы, которые объединяют различные идеи, содержащиеся в литературе:

1. трудно сформулировать единую экономическую теорию приватности, поскольку экономически значимые вопросы приватности возникают в самых разных контекстах;
2. существуют теоретические и эмпирические ситуации, когда защита частной жизни может как повысить, так и понизить благосостояние индивида и общества;
3. в цифровых экономиках способность потребителей принимать обоснованные решения о неприкосновенности частной жизни сильно затруднена, поскольку потребители часто находятся в положении несовершенной или асимметричной информации о том, когда собираются их данные, для каких целей и с какими последствиями.





◇ Google и Meta скорректировали политику работы с данными из-за вступившего ранее в силу закона ЕС о цифровых услугах (Digital Services Act, DSA).

◇ В законе предусмотрены специальные положения для «очень больших» онлайн-платформ или поисковых систем – Very Large Online Platforms (VLOP) и Very Large Search Engines (VLSE) – насчитывающих более 45 миллионов пользователей. Такие игроки должны будут ежегодно проводить широкомасштабную оценку рисков возможного негативного воздействия их сервисов, например, в вопросах доступа к нелегальным товарам, контенту или распространения дезинформации. Кроме того, VLOP и VLSE должны будут проводить всеобъемлющий анализ угроз фундаментальным правам, включая свободу самовыражения, защиту персональных данных, свободу и плюрализм средств информации в Интернете, а также права ребёнка.

◇ В этой связи в Google заявили, что внесли ряд изменений в свою политику. В частности, расширен доступ [регуляторам] к данным, касающимся ведения адресных рекламных кампаний, а также раскрыто больше информации в отношении модерирования сервисов таких, как поиск Google. В Meta сообщили о том, что Facebook и Instagram прекратили вести рекламные кампании, нацеленные на подростков, на основе активности несовершеннолетних в этих сервисах.

## 1154 В ЕС могут появиться платные версии Facebook и Instagram



◇ Meta рассматривает возможность создания нового платного уровня подписки в Facebook и Instagram, который будет предназначен для европейских пользователей. Причина – желание обойти жесткие требования регуляторов Евросоюза.

◇ Meta обычно размещает рекламу, анализируя данные пользователей, чтобы предложить им объявления, соответствующие их интересам. В ЕС у компании возникли проблемы в связи с действием Общего регламента по защите данных в интернете (GDPR).

◇ Кроме того, в Евросоюзе недавно вступил в силу Закон о цифровых услугах (DMA), который требует от таких сервисов, как Meta, предлагать контент, не использующий персональные данные людей для настройки.

◇ В Meta считают, что, предлагая платную версию Facebook и Instagram и позволяя пользователям отказаться от бесплатной рекламы, они снимут некоторые опасения регуляторов.

◇ Это уже не первый случай, когда Meta изменяет один из своих сервисов для ЕС. В настоящее время технологический гигант заблокировал доступ жителей ЕС к своему новому сервису Threads, даже при использовании VPN, из-за опасений DMA.

◇ Согласно DMA, компании Meta запрещено повторно задействовать данные пользователя, включая его имя или местоположение, в своих продуктах без специального разрешения. Например, Meta не имеет права использовать информацию, полученную о человеке из Facebook, для рекламы на Threads и наоборот.

## Microsoft с оговорками согласилась хранить ПД европейских пользователей на территории ЕС

**Silicon**  
TECHNOLOGY POWERING BUSINESS

Podcast | Audio News | Whitepapers | Workspace | Silicon

### Microsoft To Allow Cloud Users To Store Personal Data In Europe

Tom Jowitt, January 11, 2024, 2:35 pm



In effort to resolve privacy worries, Microsoft is to allow its cloud customers to store all personal data within EU

Microsoft has confirmed that it will allow cloud customers to store all their personal data within the European Union, in an effort to allay privacy concerns.

◇ Корпорация Microsoft заявила, что с рядом оговорок позволит [европейским] пользователям облачных услуг компании хранить все их персональные данные (ПД) в границах Евросоюза, сообщил в четверг silicon.co.uk.

◇ По информации издания, Microsoft таким образом хочет успокоить тех, кто тревожится по поводу сохранности личных данных европейцев.

◇ Ранее корпорация согласилась на обработку некоторых данных в Европе, теперь же на территории ЕС будет обрабатываться информация, сгенерированная автоматически при пользовании сервисами Azure, Microsoft 365, Power Platform и Dynamics 365.

◇ В то же время Microsoft предусмотрела возможность передачи некоторых ПД европейцев за пределы Евросоюза, пообещав проследить за тем, чтобы любая переданная в целях безопасности за пределы ЕС информация была задокументирована, собрана лишь в том объёме, который необходим для важных функций обеспечения кибербезопасности, и использована исключительно в указанных целях.

## Пользователи Google в ЕС получают больше возможностей контроля данных, чем остальные

◇ Google адаптирует свои методы сбора и обработки данных, чтобы соответствовать новому Европейскому Закону о цифровых рынках, который начнёт действовать 6 марта. Недавно компания предложила пользователям на территории Евросоюза выбрать, хотят ли они сохранить связь между определенными сервисами Google.

◇ Согласно нововведениям, жители ЕС смогут ограничить обработку персональных данных в таких сервисах, как поисковик Google, YouTube, рекламные службы компании, Play Маркет, Chrome, а также Google Покупки и Google Карты.

◇ Однако пользователи должны помнить, что ограничение доступа к их данным может повлиять на функциональность некоторых сервисов. Например, блокировка сбора данных в YouTube и Chrome приведёт к потере персонализированных рекомендаций, а в Google Картах не будут отображаться места на основе предыдущих активностей пользователя.

◇ «Когда эти сервисы связаны, они могут обмениваться вашими данными между собой и с другими сервисами Google в определенных целях. Между связанными сервисами Google могут передаваться любые типы данных, описанные в Политике конфиденциальности Google. К таким данным относится, в частности, история ваших действий, которая сохраняется, если вы вошли в аккаунт. Например, это может быть информация о том, что вы ищете и какие видео смотрите или слушаете», - объяснила компания в своем блоге.

◇ Пользователям предложено самостоятельно настроить список сервисов, которые могут обмениваться данными. В компании добавили, что связь сервисов Google между собой не подразумевает передачу данных сторонним продуктам или компаниям. Все взаимодействия осуществляются исключительно в рамках экосистемы Google и в соответствии с их Политикой конфиденциальности.

◇ Настройки, касающиеся сохранения связи между сервисами, вступят в силу 6 марта 2024 года. Пользователи смогут в любое время проверить и изменить список связанных сервисов.

## Итоги применения GDPR в 2018-2023гг. и дальнейшие перспективы





<b>5</b>	<b>EUROPEAN DATA PROTECTION BOARD ACTIVITIES IN 2019</b>	<b>12</b>
5.1.	<b>General guidance</b>	12
5.1.1.	Guidelines on Code of Conduct	13
5.1.2.	Guidelines on the processing of personal data in the context of online services	13
5.1.3.	Recommendation on the EDPS draft list on processing operations subject to Data Protection Impact Assessments (DPIAs)	13
5.1.4.	Guidelines on processing of personal data through video services	14
5.1.5.	Guidelines on Data Protection by Design and by Default	14
5.1.6.	Guidelines on the Right to be Forgotten	15
5.1.7.	Guidelines adopted following public consultation	15
5.2.	<b>Consistency Opinions</b>	15
5.2.1.	Opinions on the draft Data Protection Impact Assessments lists (DPIAs)	16
5.2.2.	Opinion on transfers of personal data between EEA and non-EEA Financial Supervisory Authorities	16
5.2.3.	Opinion on the interplay between ePrivacy Directive and the GDPR	16
5.2.4.	Opinion on the competence of a Supervisory Authority in case of a change in circumstances relating to the main or single establishment	16
5.2.5.	Opinions on Accreditation Criteria for monitoring bodies of Code of Conduct	17
5.2.6.	Opinion on Standard Contractual Clauses for processors by Danish SA	17
5.2.7.	Opinions on Binding Corporate Rules	18
5.3.	<b>Legislative consultation</b>	18
5.3.1.	EU-U.S. Privacy Shield	18
5.3.2.	Opinion on clinical trials Q&A	19
5.3.3.	Statement on the future ePrivacy regulation	19
5.3.4.	Additional protocol to the Budapest Convention on Cybercrime	19
5.3.5.	EDPB-EDPS Joint Opinion on the eHealth Digital Service Infrastructure	20

<b>6</b>	<b>SUPERVISORY AUTHORITY ACTIVITIES IN 2019</b>	<b>28</b>
6.1.	<b>Cross-border cooperation</b>	28
6.1.1.	Preliminary procedure to identify the Lead and Concerned Supervisory Authorities	28
6.1.2.	Database regarding cases with cross-border component	29
6.1.3.	One-Stop-Shop Mechanism	29
6.1.4.	Mutual assistance	30
6.1.5.	Joint operations	31
6.2.	<b>National cases</b>	31
6.2.1.	Some relevant national cases with exercise of corrective powers	31
6.2.1.1.	Austria	31
6.2.1.2.	Belgium	31
6.2.1.3.	Denmark	32
6.2.1.4.	Finland	32
6.2.1.5.	France	32
6.2.1.6.	Germany	33
6.2.1.7.	Greece	33
6.2.1.8.	Hungary	34
6.2.1.9.	Italy	34
6.2.1.10.	Latvia	34
6.2.1.11.	Lithuania	34
6.2.1.12.	Malta	35
6.2.1.13.	Norway	35
6.2.1.14.	Poland	35
6.2.1.15.	Romania	35
6.2.1.16.	Spain	36
6.2.1.17.	Sweden	36
6.2.1.18.	United Kingdom	37
6.3.	<b>SA survey on budget and staff</b>	37
<b>8</b>	<b>MAIN OBJECTIVES FOR 2020</b>	<b>40</b>
8.1.	<b>Legal work plan</b>	40
8.1.1.	Guidance	40
8.1.2.	Advisory role to the European Commission	40
8.1.3.	Consistency findings	41
8.2.	<b>Communications</b>	41



**PILLAR 1**

**Advancing harmonisation and facilitating compliance**

Key notions of Data Protection law:

- Guidelines on data subject rights
- Guidelines on legitimate interest

Ensuring consistency between data protection authorities

Advise the EU legislator on important data protection issues

Awareness-raising common tools on GDPR for SMEs

**PILLAR 2**

**Supporting effective enforcement and efficient cooperation between SAs**

Consistent application of GDPR cooperation mechanisms:

- Guidance on One-Stop-Shop procedures, Mutual assistance and EDPB decisions relating to dispute resolution
- Guidelines on administrative fines
- Implement a Coordinated Enforcement Framework and a Support Pool of Experts to promote solidarity between authorities and sharing of experts

**PILLAR 3**

**A fundamental rights approach to new technologies**

New technologies:

- Guidelines on the use of facial recognition technology in the area of law enforcement
- Guidelines on Blockchain
- Guidelines on anonymisation and pseudonymisation
- EPrivacy Regulation

**PILLAR 4**

**The global dimension**

Promote high standards for international data transfers:

- Adequacy decisions (both under GDPR and LED)
- Codes of Conduct and certification as tools for international transfers

## LES CHIFFRES CLÉS 2021

### CONSEILLER & RÉGLEMENTER

22 AUDITIONS PARLEMENTAIRES

13 QUESTIONNAIRES ADRESSÉS AU PARLEMENT OU À UN PARLEMENTAIRE EN MISSION

154 DÉLIBÉRATIONS DONT 121 AVIS SUR DES PROJETS DE TEXTE

576 DOSSIERS D'AUTORISATION EN SANTÉ TRAITÉS DONT 54 AUTORISATIONS DE RECHERCHE SUR LA COVID-19

### ACCOMPAGNER LA CONFORMITÉ

81 393 ORGANISMES ONT DÉSIGNÉ UN DÉLÈGUE À LA PROTECTION DES DONNÉES (DPO)

28 810 DPO DÉSIGNÉS

**+13%** PAR RAPPORT À 2020

123 882 COMPTES CRÉÉS SUR LE MOOD® ATELIER RGPD®

5 037 **+79%** NOTIFICATIONS DE VIOLATIONS DE DONNÉES

Moins d'un tiers des Comptes créés de formation à distance (CFD) réglementés par la protection des données.

### PROTÉGER

14 143 PLAINTES QUI ONT CONDUIT À

5 848 RÉPONSES RAPIDES

8 295 ÉTUDES PLUS APPROFONDIES

12 522 PLAINTES CLÔTURÉES

5 329 DEMANDES VALABLES DE DROIT D'ACCÈS INDIRECT (DAI)

3 960 VÉRIFICATIONS EFFECTUÉES

## INFORMER

161 475 APPELS REÇUS **+33%**

16 898 REQUÊTES REÇUES PAR VOIE ÉLECTRONIQUE

10 809 884 VISITES SUR LES SITES WEB DE LA CNIL **+12%**

130 800 FOLLOWERS SUR TWITTER **+5%**

43 724 FANS SUR FACEBOOK **+17%**

153 732 ABONNÉS SUR LINKEDIN **+16%**

### CONTRÔLER & SANCTIONNER

384 CONTRÔLES ONT ÉTÉ EFFECTUÉS DONT

118 CONTRÔLES SUR PLACE	65 CONTRÔLES SUR PIÈCE
173 CONTRÔLES EN LIGNE	28 CONTRÔLES SUR ADDITION

135 MISES EN DEMEURE DONT 3 PUBLIQUES

45 RAPPELS À L'ORDRE DE LA PRÉSIDENTE


18 SANCTIONS DONT

15 AMENDES POUR UN MANQUANT LÉGÈRE DE 214 106 000 EUROS SONT ÉMISSES À DES ALIQUOTES TRÈS ÉLEVÉES	2 RAPPELS À L'ORDRE DE LA FORMATION PLURIPARTISANNE AVEC ALIQUOTES
	1 LIQUIDATION INSTAURÉE

**+17** projets de sanctions européens examinés par la CNIL

### RESSOURCES HUMAINES

BUDGET 21,8 MILLIONS D'EUROS



36% 64%

245 emplois

39 ans Âge moyen

81% DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A

59% D'AGENTS ARRIVÉS ENTRE 2016 ET 2021

8 ANS ANCIENNETÉ MOYENNE DES AGENTS DE LA CNIL





## Сообщение Европейской комиссии в адрес Европейского парламента и Совета Европы о текущей практике GDPR



Сообщение «Защита персональных данных как основа расширения прав и возможностей граждан и подход ЕС к цифровой трансформации - два года применения Общего положения о защите данных» содержит в себе некоторые интересные моменты:

- в 2018-20 годах штат национальных надзорных органов вырос на 42%, а бюджет на 49%, но при этом показатель роста сильно отличается в разных государствах-членах ЕС;
- планируется обновление SCC, а также разработка руководства по сертификации от EDPB;
- почти все государства-члены ЕС (за исключением Словении) гармонизировали свое национальное законодательство с требованиями GDPR.

## Права, предоставленные субъектам, не всегда используются во благо

### Ст.15 GDPR: Право на доступ

- Amazon отправил 1700 голосовых записей Alexa не тому пользователю после запроса данных. ([The Verge](#))
- Злоумышленник взломал аккаунт Spotify и получил все сведения о владельце аккаунта, просто запросив их. ([Jean Yang](#))

### Ст.17 GDPR: Право быть забытым

- Google пришлось исключить из поисковой выдачи сведения о голландском докторе, который был уволен из-за плохого ухода за пациентом. ([NYT](#))
- Французский мошенник Майкл Франсуа Буджалдон попытается удалить из Интернета любые сведения о судебном разбирательстве против себя, ранее рассмотренным в окружном суде США. ([PlainSite](#))
- СМИ США регулярно получают запросы на удаление статей о судебных процессах в США, касающихся мошенничества, совершенного европейцами. ([Mike Masnick](#))

### Ст.20 GDPR: Право на переносимость данных

- Если вы можете перенести свои данные из Facebook в другие приложения, то вы можете сделать то же самое в обратном направлении. И кто же будет иметь преимущество: Facebook или его конкуренты? ([Ben Thompson](#))
- Способы и формы реализации права на переносимость данных, в качестве некоего отраслевого стандарта, могут быть навязаны лидерами отрасли для всех остальных компаний, включая стартапы. ([Tyler Cowen](#))

### Ст.21 GDPR: Право отказаться (opt out) от обработки данных

- Запрет компаниям ограничивать предоставление услуг или повышать на них цены для потребителей, которые отказываются от обмена своими персональными данными, поощряет таких потребителей (free riders) и сокращает доступ к бесплатному контенту и услугам для всех остальных. ([ITIF](#))

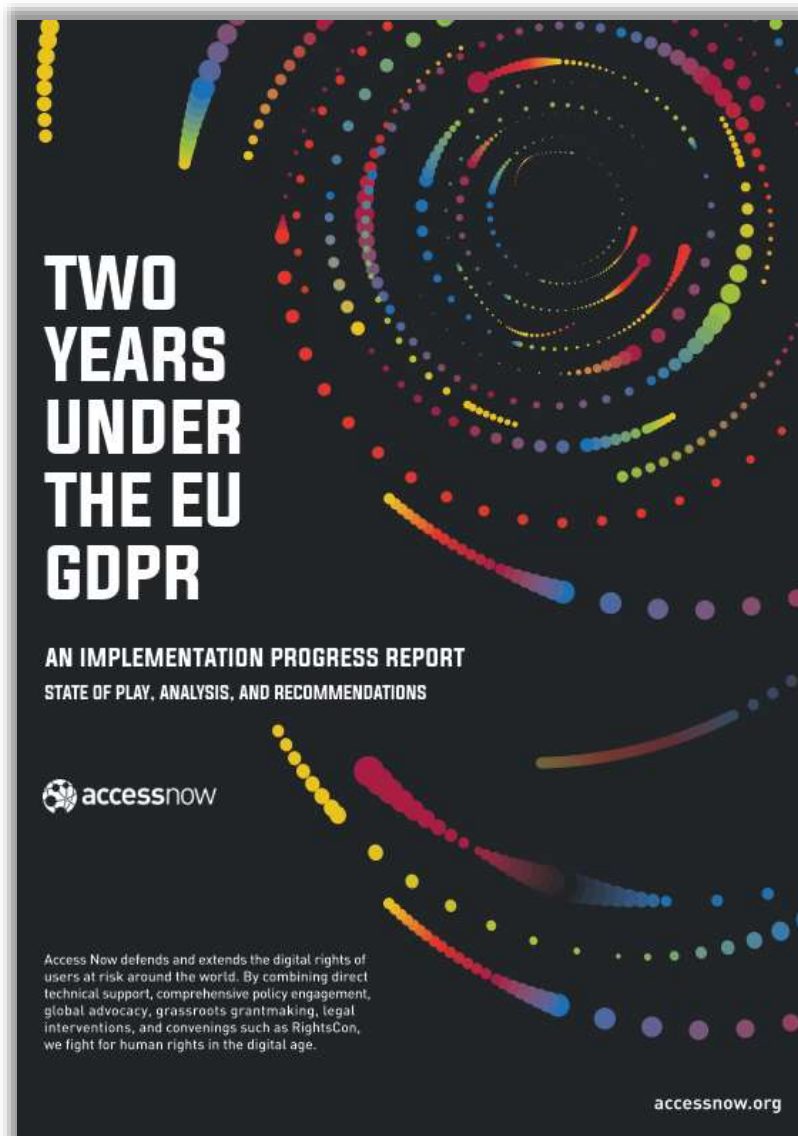
## Доклад экспертной группы (Multistakeholder Expert group) об итогах применения GDPR в 2018-2019 годах

- Могут ли несовершеннолетние давать согласие или это должны быть их родители - часто неясно. Это может привести к отказу в предоставлении услуг детям и к тому, что дети не смогут выходить в Интернет до тех пор, пока они не достигнут определенного возраста, что не является целью, которую преследует GDPR. (стр. 10)
- Cookie-баннеры, размещаемые на веб-сайтах, часто дают неоднозначную информацию и заставляют пользователей давать согласие на обработку и обмен данными с неопределенными третьими лицами в целях таргетированной рекламы. (стр. 10)
- Член (собрания) сообщает об увеличении числа лиц, желающих подать иск в суд для защиты прав субъектов данных. (стр. 11)
- Некоммерческие организации, имеющие право на защиту прав субъектов данных в соответствии со статьей 80 GDPR, начали использовать возможность осуществлять представительские действия по нарушениям GDPR. (стр. 12)
- Некоторые члены считают, что применение GDPR к новым технологиям, таким как блокчейн, большие данные или искусственный интеллект, вызывает вопросы, которые, если их не решить, могут повлиять на развитие таких технологий. (стр. 16)
- Рынок для опытных DPO все еще незрел, и в этой области все еще слишком мало экспертов, принимающих во внимание актуальные потребности организаций. CEDPO (Confederation of the European Data Protection Organisations) обозначает обеспокоенность в связи с появлением множества учебных курсов, которые, как утверждается, позволят неспециалистам стать DPO за очень короткий период времени, что нанесет серьезный ущерб профессии в области защиты данных. По их мнению, есть лица, выступающие в качестве DPO, которые не обладают необходимым опытом. (стр. 17)
- В свете возросшей сложности закона о защите данных, сопровождаемого режимом жестких санкций, наблюдается тенденция к переносу большей части рабочей нагрузки по защите данных в юридический отдел, в то время как DPO остается ответственным за минимальный набор обязательств, указанных в GDPR. (стр. 17)

**1165 Отчет Datenschutzkonferenz об итогах применения GDPR в 2018-2019гг.**

Relevant provision of GDPR	Proposed amendment, plus brief explanation
Article 4	The GDPR currently lacks a definition of "anonymization". It would be useful in practice and it should be aligned with the requirements set out in Opinion 05/2014 on Anonymization Techniques.
Articles 13 and 14	The categories listed in paragraph 2 of Article 13 and paragraph 2 of Article 14 of the GDPR should be aligned by including the information referred to in point (b) of Article 14(2) in paragraph 2 of Article 13 rather than in paragraph 1.
Article 18(1)	Right to restriction of processing: In addition to the grounds listed in points (a) to (d) of Article 18(1) of the GDPR, the right to restriction of processing should also apply to those cases in which the requisite erasure is not carried out only because the data need to be retained pursuant to point (b) of Article 17(3) of the GDPR in order to comply with retention periods.
Article 21(2)	Right to object to direct marketing: The words "in addition to the right to object under paragraph 1" should be inserted to make it clear that paragraph 2 does not represent a sub-case of paragraph 1, but that, in contrast to paragraph 1, it also applies when data are not processed on the basis of points (e) and (f) of Article 6(1) of the GDPR.
Article 24(2)	It appears that the wording in Article 24(2) of the GDPR could lead to misunderstandings. The German version should be aligned to the English version by replacing "Anwendung" (application) with "Einführung" (implementation) and "Datenschutzvorkehrungen" (data protection provisions) with "Datenschutzschutzregelwerke" (data protection policies).
Article 27	A duty to publish the representative's contact details should be introduced in Article 27 of the GDPR in analogy with Article 37(7) of the GDPR (data protection officer), as in many cases it is unclear whether the controller/processor has met its duty to appoint a representative and where that representative is based.
Article 40(4), Article 41(1) and (4)	Clarification as to whether the establishment of an accredited supervisory body is obligatory (in analogy with the Board's guidelines of 12 Feb. 2019) or only optional.

Отчет об опыте, полученном в Германии в ходе применения GDPR в 2018-2019 годах, был подготовлен Конференцией независимых федеральных и государственных надзорных органов Германии по защите данных (Datenschutzkonferenz (DSK)) и принят на ее 98-й конференции 6 ноября 2019 года. Публикуя этот отчет, DSK хотел бы включить этот опыт в процесс оценки и анализа, требуемый в соответствии со статьей 97 GDPR, и, после этого, внести предложения по улучшению некоторых положений GDPR для оптимизации правоприменительной практики.



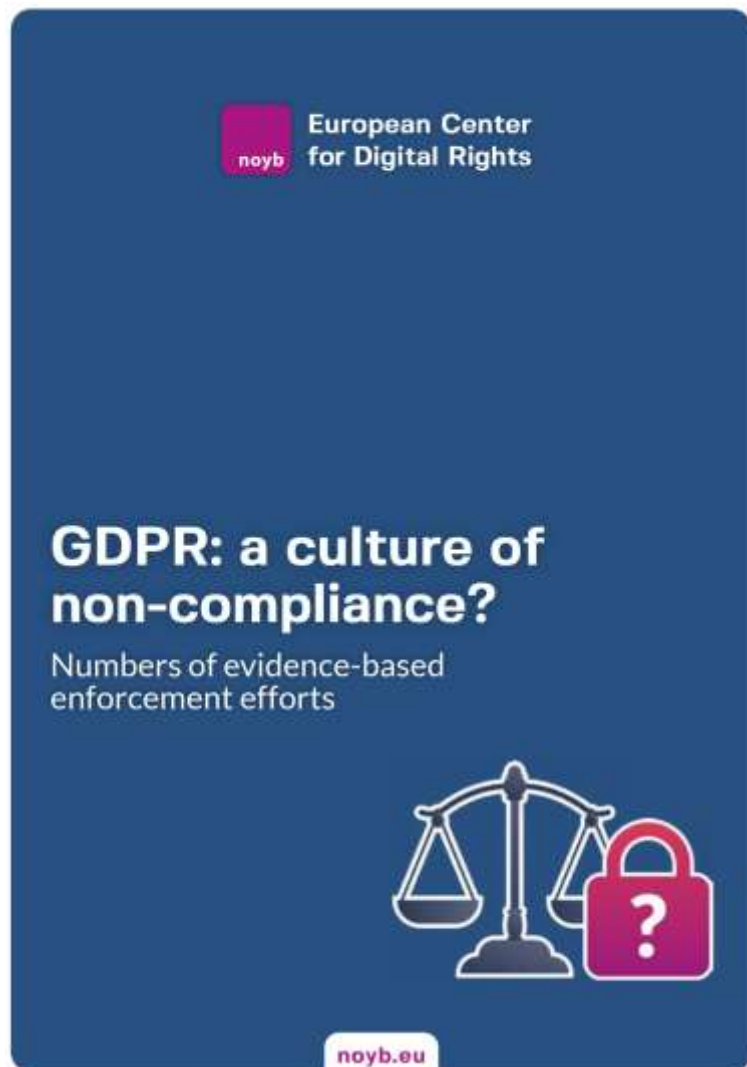
В отчёте Access Now «Two years under the EU GDPR» обозначены следующие ключевые моменты:

- за два года регуляторы наложили 231 штрафа, а получено было 144 376 жалоб субъектов;
- из 30 регуляторов из 27 стран ЕС только 9 довольны уровнем своего ресурсного обеспечения;
- в Польше, Румынии, Венгрии и Словакии суды и власть злоупотребляют GDPR, чтобы ограничить журналистские расследования;
- GDPR показал себя надежным инструментом для регулирования обработки данных с отношении должностных лиц и органов общественного здравоохранения. Но решение Венгрии ограничить применение GDPR во время пандемии Covid-19 нарушает права субъектов на защиту данных;
- проблемы правоприменения GDPR и настойчивое стремление УК снизить текущие стандарты защиты данных в ходе переговоров по Brexit могут иметь негативные последствия для любых будущих переговоров о так называемом решении об адекватности между ЕС и Великобританией в части передачи данных между двумя юрисдикциями.

1167 Отчет ComplyCloud правоприменении GDPR в 2018-2023гг.



<https://www.complycloud.com/eu-casebook/>  
<https://ciso2ciso.com/wp-content/uploads/2023/10/EU-GDPR0ACasebook-2023.pdf>



⬇ Эксперты утверждают, что высокие штрафы и репутация являются основными факторами, убеждающими руководство в необходимости соблюдения GDPR.

⬇ Рекомендации, руководства и "неформальные" решения оказывают мало влияния.

⬇ В целом сохраняется давление на приоритет бизнес-интересов над соблюдением закона.

⬇ B2B-клиенты и поставщики из ЕС не представляют большой проблемы, но поставщики вне ЕС вызывают большую головную боль для внутренних экспертов.

⬇ Внутренние эксперты призывают к более серьезному правоприменению и четким судебным решениям.



## 1169 Подготовка позиции Европейской комиссии по обновлению GDPR

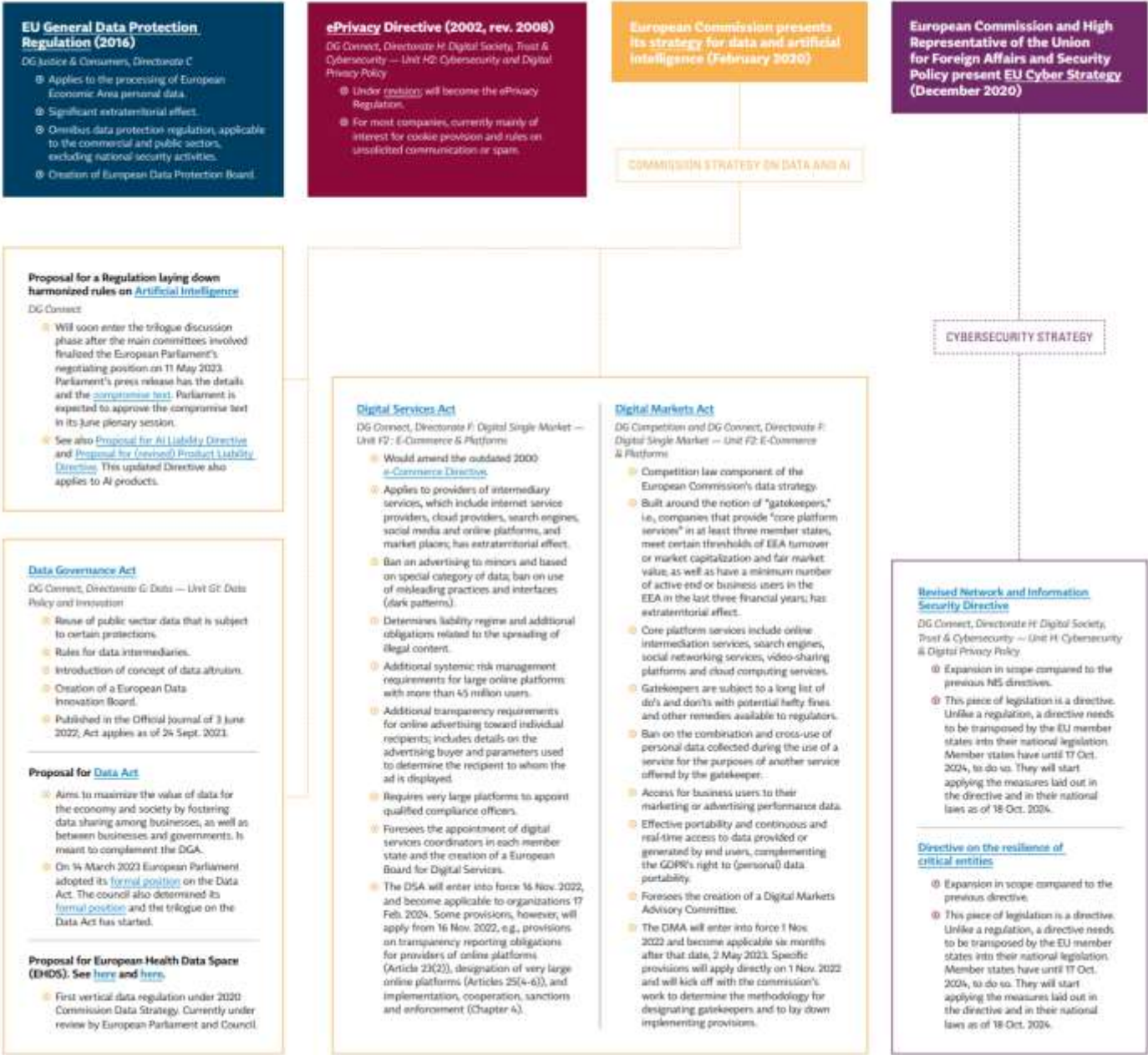
В соответствии со ст.97 GDPR 25 мая 2020 года и каждые четыре года впоследствии Европейская комиссия должна направлять отчет об оценке и пересмотре GDPR в Европейский парламент и Совет ЕС. Сам отчет также должен быть опубликован. В октябре 2019 года был опубликован проект такого отчета, в котором можно выделить следующие аспекты:

- Германия указала на противоречивость и фрагментарность правоприменительной практики GDPR, а Чехия предложила обобщить и опубликовать описание лучших практик;
- Ирландия охарактеризовала подход GDPR к защите детей как фрагментированный и разрозненный, а Франция и Нидерланды требуют установления единого возраста согласия в ЕС;
- Германия и Чехия хотят, чтобы EDPB подготовило единый реестр процессов обработки данных, для которых DPIA (ст.35 GDPR) будет обязательным;
- Германия отметила, что компании хотели бы более быстрой и конкретной помощи со стороны DPA, а субъектам требуется больше советов по Privacy и ускорения обработки своих запросов;
- Германия предложила разработать единые критерии в отношении наложения штрафов;
- Литва предложила уточнить обязательность исполнения судебного решения для DPA, находящегося в другой юрисдикции;
- Болгария и Германия обратили внимание на перегруженность DPA в подготовке ответов на жалобы субъектов в связи с утечками (89,000 на апрель 2019 г.) их данных (ст.33 и ст.77 GDPR);
- Нидерланды представили список стран – потенциальных будущих кандидатов на признание в качестве обеспечивающих адекватный уровень защиты (ст.45(3) GDPR). К ним относятся Сингапур, Колумбия, Мексика, Южная Африка, Сербия и Международный финансовый центр Дубая, а также все страны, которые ратифицировали и внедрили модернизированную Конвенцию 108+;
- Бельгия указала на нежелание применять кодексы поведения (ст.40 GDPR) из-за отсутствия четких руководящих принципов, Болгария назвала кодексы поведения способом получения организациями «индальгенции» в отношении нарушений GDPR, а Нидерланды поставили под сомнение положения интерпретации EDPB в отношении норм GDPR о кодексах поведения;
- Бельгия заявила, что использование обязательных корпоративных правил (ст.47 GDPR), противоречит целям гармонизации применения GDPR.

## Законодательные инициативы о персональных данных в ЕС и США



# 1171 Актуальные инициативы по регулированию оборота данных в ЕС на 05.2023



**EU General Data Protection Regulation (2016)**  
 DG Justice & Consumers, Directorate C

- Applies to the processing of European Economic Area personal data.
- Significant extraterritorial effect.
- Omnibus data protection regulation, applicable to the commercial and public sectors, excluding national security activities.
- Creation of European Data Protection Board.

**ePrivacy Directive (2002, rev. 2008)**  
 DG Connect, Directorate H: Digital Society, Trust & Cybersecurity — Unit H2: Cybersecurity and Digital Privacy Policy

- Under revision; will become the ePrivacy Regulation.
- For most companies, currently mainly of interest for cookie provision and rules on unsolicited communication or spam.

**European Commission presents its strategy for data and artificial intelligence (February 2020)**

COMMISSION STRATEGY ON DATA AND AI

**European Commission and High Representative of the Union for Foreign Affairs and Security Policy present EU Cyber Strategy (December 2020)**

CYBERSECURITY STRATEGY

**Proposal for a Regulation laying down harmonized rules on Artificial Intelligence**  
 DG Connect

- Will soon enter the trilogue discussion phase after the main committees involved finalized the European Parliament's negotiating position on 11 May 2023. Parliament's press release has the details and the [corporate law](#). Parliament is expected to approve the compromise text in its June plenary session.
- See also [Proposal for AI Liability Directive](#) and [Proposal for \(revised\) Product Liability Directive](#). This updated Directive also applies to AI products.

**Digital Services Act**  
 DG Connect, Directorate F: Digital Single Market — Unit F2: E-Commerce & Platforms

- Would amend the outdated 2000 e-Commerce Directive.
- Applies to providers of intermediary services, which include internet service providers, cloud providers, search engines, social media and online platforms, and market places; has extraterritorial effect.
- Ban on advertising to minors and based on special category of data; ban on use of misleading practices and interfaces (dark patterns).
- Determines liability regime and additional obligations related to the spreading of illegal content.
- Additional systemic risk management requirements for large online platforms with more than 45 million users.
- Additional transparency requirements for online advertising toward individual recipients; includes details on the advertising buyer and parameters used to determine the recipient to whom the ad is displayed.
- Requires very large platforms to appoint qualified compliance officers.
- Foresees the appointment of digital services coordinators in each member state and the creation of a European Board for Digital Services.
- The DSA will enter into force 16 Nov. 2022, and become applicable to organizations 17 Feb. 2024. Some provisions, however, will apply from 16 Nov. 2022, e.g., provisions on transparency reporting obligations for providers of online platforms (Article 23(2)), designation of very large online platforms (Articles 25(4)-(6)), and implementation, cooperation, sanctions and enforcement (Chapter 4).

**Digital Markets Act**  
 DG Competition and DG Connect, Directorate F: Digital Single Market — Unit F2: E-Commerce & Platforms

- Competition law component of the European Commission's data strategy.
- Built around the notion of "gatekeepers," i.e., companies that provide "core platform services" in at least three member states, meet certain thresholds of EEA turnover or market capitalization and fair market value, as well as have a minimum number of active end or business users in the EEA in the last three financial years; has extraterritorial effect.
- Core platform services include online intermediation services, search engines, social networking services, video-sharing platforms and cloud computing services.
- Gatekeepers are subject to a long list of do's and don'ts with potential hefty fines and other remedies available to regulators.
- Ban on the combination and cross-use of personal data collected during the use of a service for the purposes of another service offered by the gatekeeper.
- Access for business users to their marketing or advertising performance data.
- Effective portability and continuous and real-time access to data provided or generated by end users, complementing the GDPR's right to (personal) data portability.
- Foresees the creation of a Digital Markets Advisory Committee.
- The DMA will enter into force 1 Nov. 2022 and become applicable six months after that date, 2 May 2023. Specific provisions will apply directly on 1 Nov. 2022 and will kick off with the commission's work to determine the methodology for designating gatekeepers and to lay down implementing provisions.

**Data Governance Act**  
 DG Connect, Directorate G: Data — Unit G: Data Policy and Innovation

- Reuse of public sector data that is subject to certain protections.
- Rules for data intermediaries.
- Introduction of concept of data altruism.
- Creation of a European Data Innovation Board.
- Published in the Official Journal of 3 June 2022; Act applies as of 24 Sept. 2023.

**Proposal for Data Act**

- Aims to maximize the value of data for the economy and society by fostering data sharing among businesses, as well as between businesses and governments. It is meant to complement the DGA.
- On 14 March 2023 European Parliament adopted its [formal position](#) on the Data Act. The Council also determined its [formal position](#) and the trilogue on the Data Act has started.

**Proposal for European Health Data Space (EHDS). See [here](#) and [here](#).**

- First vertical data regulation under 2020 Commission Data Strategy. Currently under review by European Parliament and Council.

**Revised Network and Information Security Directive**  
 DG Connect, Directorate H: Digital Society, Trust & Cybersecurity — Unit H: Cybersecurity & Digital Privacy Policy

- Expansion in scope compared to the previous NIS directives.
- This piece of legislation is a directive. Unlike a regulation, a directive needs to be transposed by the EU member states into their national legislation. Member states have until 17 Oct. 2024, to do so. They will start applying the measures laid out in the directive and in their national laws as of 18 Oct. 2024.

**Directive on the resilience of critical entities**

- Expansion in scope compared to the previous directive.
- This piece of legislation is a directive. Unlike a regulation, a directive needs to be transposed by the EU member states into their national legislation. Member states have until 17 Oct. 2024, to do so. They will start applying the measures laid out in the directive and in their national laws as of 18 Oct. 2024.

## 1172 Proposal 2017/0003: GDPR для электронных коммуникаций




[Proposal 2017/0003 \(COD\) for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC \(Regulation on Privacy and Electronic Communications\)](#)

Проект Регламента об уважении к частной жизни и защите персональных данных в области электронных коммуникаций, а также об отмене директивы 2002/58/EC (Положение о конфиденциальности и электронных коммуникациях).

### Полезные ссылки:

- [Общее описание целей, задач, структуры и содержания проекта](#)
- [Анализ EDPB по соотношению норм GDPR и ePR](#)

## Оптимизация сотрудничества между национальными ДПА при обеспечении соблюдения GDPR


 REF: AWD(2023) 27680 - 24032023

regulation	
CALL FOR EVIDENCE FOR AN INITIATIVE (without an impact assessment)	
This document aims to inform the public and stakeholders about the Commission's work, so they can provide feedback and participate effectively in consultation activities. We ask these groups to provide views on the Commission's understanding of the problem and possible solutions, and to give us any relevant information they may have. <b>!</b> You should finalise this document at the earliest stages of the preparatory process, so that best use can be made of feedback from stakeholders.	
<b>TITLE OF THE INITIATIVE</b>	General Data Protection Regulation – procedural rules on enforcement
<b>LEAD DG – RESPONSIBLE UNIT</b>	JUST C3 Data protection
<b>Likely type of initiative</b>	Proposal for a Regulation
<b>INDICATIVE TIMING</b>	Q2-2022
<b>ADDITIONAL INFORMATION</b>	<a href="https://commission.europa.eu/law/law-topic/data-protection/data-protection-60_en">https://commission.europa.eu/law/law-topic/data-protection/data-protection-60_en</a>
<b>A. Political context, problem definition and subsidiarity check</b>	
<b>Political context</b>	
The General Data Protection Regulation (GDPR) is an important component of the human-centric approach to technology and a compass for the use of technology in the green and digital transitions of the EU economy and society. It sets a framework for initiatives under the <a href="#">EU's data strategy</a> and ensures they are designed to effectively empower individuals.  This initiative would support the robust enforcement of the GDPR. It is included in the Commission's <a href="#">2023 work programme</a> (under the general heading "A new push for European Democracy"). It follows the Commission's <a href="#">report on the application of the GDPR</a> , which highlighted that there was room for improvement regarding procedures applied by national data protection supervisory authorities when dealing with cross-border cases.  In addition, the initiative responds to a <a href="#">letter</a> that the European Data Protection Board (EDPB) officially transmitted to the Commission in October 2022, identifying procedural aspects of the cooperation between national data protection supervisory authorities in cross-border cases that could be harmonised at EU level.	
<b>Problem the initiative aims to tackle</b>	
The initiative aims to streamline cooperation between national data protection supervisory authorities when enforcing the General Data Protection Regulation (GDPR) in cross-border cases. To this end, the initiative proposes to harmonise some aspects of the administrative procedures that are applied by data protection supervisory authorities in these cases.  Since the entry into application of the GDPR in May 2018, divergences have become apparent in approaches followed by the national data protection supervisory authorities on issues such as: <ul style="list-style-type: none"> <li>• complaint handling</li> <li>• the form of complaints</li> <li>• duration of proceedings</li> <li>• the extent of the right to be heard and the moment in the procedure when it is granted</li> <li>• the involvement of complainants during the procedure, including the provision of information on the progress of the investigation.</li> </ul> The GDPR set up a dispute resolution mechanism for when data protection supervisory authorities fail to reach a consensus in a cross-border case (Article 65 GDPR). To help the investigation to be resolved more quickly for both data subjects and the parties under investigation, this initiative will further spell out steps for cooperation in	

Европейская комиссия 16.02.2023 заявила инициативу, уточняющую процедурные правила, связанные с исполнением GDPR. Инициатива, которая находится в стадии подготовки, направлена на оптимизацию сотрудничества между национальными органами по защите данных при обеспечении соблюдения GDPR в трансграничных случаях.

Инициатива предусматривает гармонизацию некоторых аспектов административной процедуры, применяемой национальными органами по защите данных в трансграничных делах, что будет способствовать бесперебойному функционированию механизмов сотрудничества и разрешения споров в рамках GDPR. Кроме того, инициатива предлагает регламент, который, как ожидается, будет принят Комиссией во втором квартале 2023 года.

## В Евросоюзе хотят ужесточить законодательство против облачных сервисов США



◇ Власти ЕС планируют ужесточить правила в сфере кибербезопасности для американских компаний и поставщиков облачных сервисов — Amazon, Google, Microsoft; в соответствии с новыми предложениями в этой сфере, эти компании смогут получить сертификат кибербезопасности ЕС только совместно с базирующейся в Евросоюзе компанией.

◇ Ранее агентство ЕС по кибербезопасности (ENISA) предложило ввести систему сертификации в Евросоюзе, в рамках которой устанавливаются требования для поставщиков облачных сервисов. В частности, штаб-компания должна располагаться в стране-члене ЕС.

◇ Более жесткие правила будут в том числе применяться к "персональным и не персональным данным особой важности", нарушение которых может оказать негативное влияние на общественный порядок, общественную безопасность, жизнь или здоровье людей или защиту интеллектуальной собственности. Все имеющие доступ к данным ЕС сотрудники должны проживать на территории Евросоюза и проходить особый контроль для работы с информацией из ЕС. Все данные клиентов предлагается хранить и обрабатывать в Европе, без трансграничной передачи.



Assembly Bill No. 375

CHAPTER 55

An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy.

[Approved by Governor June 28, 2018. Filed with Secretary of State June 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

AB 375, Chau. Privacy: personal information: businesses.

The California Constitution grants a right of privacy. Existing law provides for the confidentiality of personal information in various contexts and requires a business or person that suffers a breach of security of computerized data that includes personal information, as defined, to disclose that breach, as specified.

This bill would enact the California Consumer Privacy Act of 2018. Beginning January 1, 2020, the bill would grant a consumer a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared. The bill would require a business to make disclosures about the information and the purposes for which it is used. The bill would grant a consumer the right to request deletion of personal information and would require the business to delete upon receipt of a verified request, as specified. The bill would grant a consumer a right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of 3rd parties to which the information was sold or disclosed. The bill would require a business to provide this information in response to a verifiable consumer request. The bill would authorize a consumer to opt out of the sale of personal information by a business and would prohibit the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer's data. The bill would authorize businesses to offer financial incentives for collection of personal information. The bill would prohibit a business from selling the personal information of a consumer under 16 years of age, unless affirmatively authorized, as specified, to be referred to as the right to opt in. The bill would prescribe requirements for receiving, processing, and satisfying these requests from consumers. The bill would prescribe various definitions for its purposes and would

## The California Consumer Privacy Act of 2018

**28.06.2018** в штате Калифорния (США) был принят закон о защите персональных данных потребителей. В соответствии с новым законом калифорнийские потребители смогут контролировать сбор и последующую обработку своих персональных данных.

Новый закон штата Калифорнии во многом похож на GDPR, но идет дальше и позволяет потребителям отказаться от ранее предоставленного согласия на обработку своих персональных данных, при этом обязывая провайдеров онлайн-сервисов и социальных сетей продолжать оказывать услуги в адрес таких лиц.

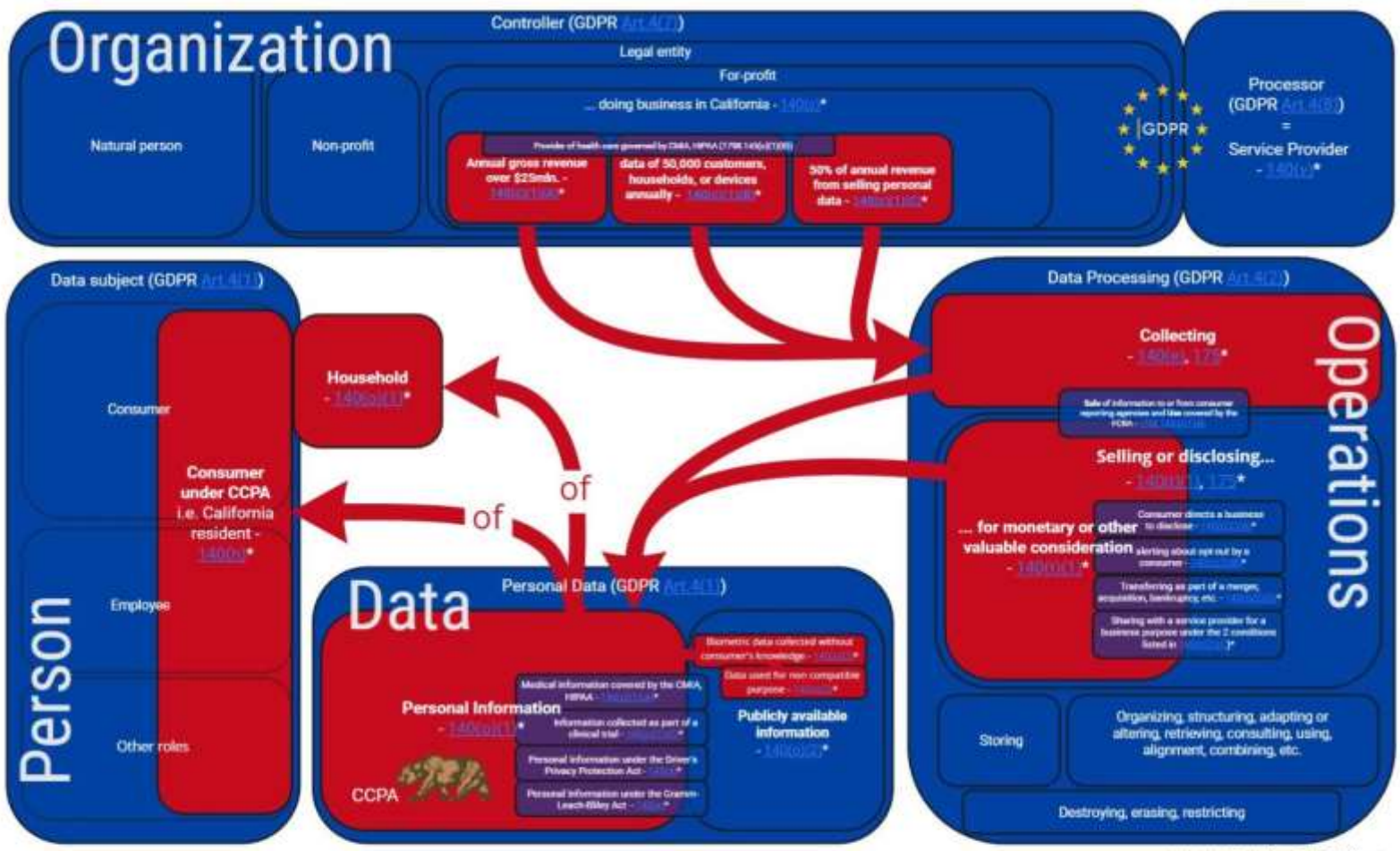
Новый закон вступил в силу **01.01.2020** и распространяется на крупные компании, которые соответствуют хотя бы одному из следующих условий:

- годовой оборот от 25 млн. долл. США;
- обработка для коммерческих целей персональных данных 50,000 или более потребителей;
- доля дохода от обработки персональных данных для коммерческих целей составляет от 50 %.

[Сравнительный анализ GDPR и CCPA от DataGuidance.](#)

1176 Область действия CCPA в сравнении с GDPR

CCPA Scope compared to GDPR



I used this combination of Venn diagram and Flow chart to express how the CCPA scope is narrower/broader comparing to the GDPR. The size of shapes does not represent the quantity of individuals, data, organizations, or operations.

Version: 3.3 2020/01  
 You can ask questions here:  
[data-privacy-office@ccpa.com](mailto:data-privacy-office@ccpa.com) or <https://www.ccprights.org>

© Siarhei Varankevich CIPP/E, CIPM, MBA. 2020



**HOW TO READ THE DIAGRAM**

CCPA APPLIES to your company if you get in a **red** sector on EACH side of the diagram.

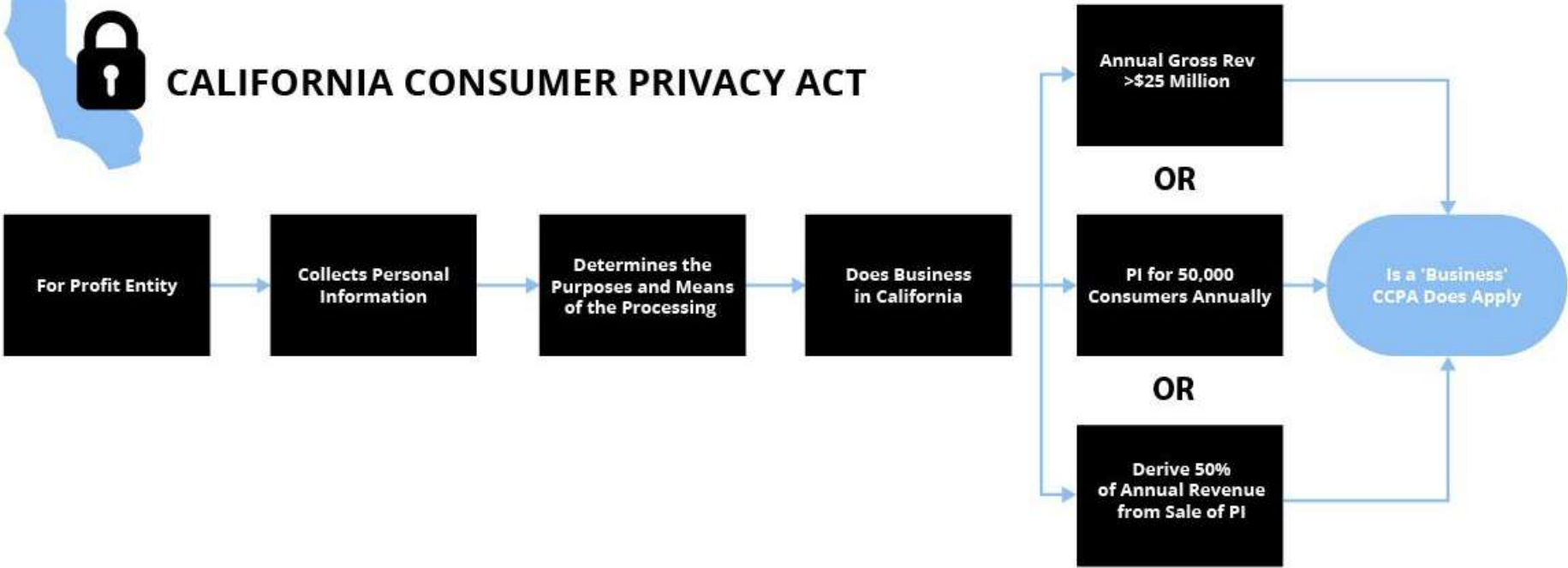
- - Covered by the CCPA
- - Not covered by the CCPA, but within the GDPR scope in the EU.

\* It refers to Cal. Civ. Code § 1798.xxx.





# CALIFORNIA CONSUMER PRIVACY ACT



THE  
NATIONAL LAW REVIEW

PUBLISH / ADVERTISE WITH US ▾ TRENDING LEGAL NEWS ▾ ABOUT US ▾ CONTACT US ▾ QUICK L

### BREAKING: Californians for Consumer Privacy Introduces California Privacy Rights Act for November 2020 Ballot

Tuesday, May 5, 2020

On May 4, 2020, Californians for Consumer Privacy (the group behind the ballot initiative that inspired the California Consumer Privacy Act of 2018 (“CCPA”)) **announced** that it had collected over 900,000 signatures to qualify the **California Privacy Rights Act** (“CPRA”) for the November 2020 ballot. The group announced that it was taking steps to submit the CPRA for inclusion on the November ballot in counties across California. The CPRA would amend the CCPA to create new and additional privacy rights and obligations in California, including the following:

- **Sensitive Personal Information.** The CPRA would establish a new category of “sensitive personal information,” which would be defined to include a Social Security Number, driver’s license number, passport number, financial account information, precise geolocation, race, ethnicity, religion, union membership, personal communications, genetic data, biometric or health information, and information about sex life or sexual orientation. The CPRA would also give consumers certain new rights around the use of “sensitive personal information.”
- **Right of Correction.** The CPRA would grant California consumers the right to request the correction of their personal information held by a business if that information is inaccurate.
- **Children’s Data.** The CPRA purports to enhance children’s privacy by tripling fines for violations of the CCPA’s opt-in to sale right and creating a new requirement to obtain opt-in consent to sell or share data from consumers under the age of 16.

4 мая 2020 года инициативная группа «Калифорнийцы за конфиденциальность потребителей», которая ранее стояла за инициативой утверждения Калифорнийского закона о защите приватности потребителей 2018 года, объявила о сборе более 900,000 подписей для инициации рассмотрения законопроекта о приватности в Калифорнии (CPRA) в ноябре 2020 года. Группа заявила, что предпринимает шаги, чтобы представить CPRA для включения в ноябрьское голосование в округах по всей Калифорнии. CPRA призван внести изменения в CCPA, которые должны предоставить субъектам данных новые права в отношении защиты их данных, включая следующие:

- дополнительная защита «чувствительных» персональных данных;
- дополнительная защита данных детей;
- право субъекта на исправление данных;
- уточненная юридическая ответственность за нарушение безопасности данных;
- создание надзорного органа по защите данных в Калифорнии.

CPRA начнёт действовать с 01.01.2023г., а к юридической ответственности за его нарушение начнут привлекать с 01.07.2023г. с периодом ретроспективного анализа с 01.01.2022г.

## 1179 The American Data Privacy and Protection Act

FCW

JUNE 6, 2022

The American Data Privacy and Protection Act stands to improve American users' data privacy and offers federal regulatory power.

A team of bipartisan lawmakers unveiled new data privacy legislation that stands to finally implement a federal set of regulations to protect Americans' online information.

Led by Reps. Frank Pallone, D-N.J., and Cathy McMorris Rodgers, R-Wash., as well as Sen. Roger Wicker, R-Miss., the bill, titled the American Data Privacy and Protection Act, has an **exhaustive list** of definitions that work to give online users power over how their data is accessed and shared by host platforms and third party data brokers.

"This bipartisan and bicameral effort to produce a comprehensive data privacy framework has been years in the making, and the release of this discussion draft represents a critical milestone," the lawmakers said in **prepared remarks**. "In the coming weeks, we will be working with our colleagues on both sides of the aisle to build support and finalize this standard to give Americans more control over their personal data. This landmark agreement represents the sum of years of good faith efforts by us, other Members, and numerous stakeholders as we work together to provide American consumers with comprehensive data privacy protections."

Двухпартийный законопроект о защите персональных данных американцев в Интернете (The American Data Privacy and Protection Act) представлен в Конгрессе Соединённых Штатов.

- Законопроект предполагает обязать онлайн-платформы и иных лиц (организации под юрисдикцией FTC, телеком-операторы и НКО), которые хранят пользовательские данные, недвусмысленно запрашивать у пользователя разрешение для доступа к персональным данным «понятным языком».
- У интернет-пользователей и потребителей должна быть возможность отказаться от просмотра таргетированной рекламы, и отдельно предусматривает усиление защиты данных несовершеннолетних лиц.
- Обеспечивать соблюдение положений закона в случае его принятия будет Федеральная торговая комиссия США (Federal Trade Commission, FTC).

## Федеральная комиссия по связи США предложила обязать операторов сообщать об утечках данных «незамедлительно»

Federal Communications Commission	FCC 22-102	
Before the Federal Communications Commission Washington, D.C. 20554		
In the Matter of	)	
Data Breach Reporting Requirements	)	WC Docket No. 22-21
<b>NOTICE OF PROPOSED RULEMAKING</b>		
Adopted: December 28, 2022	Released: January 6, 2023	
Comment Date: 30 days after publication in the Federal Register		
Reply Comment Date: 60 days after publication in the Federal Register		
By the Commission:		
<b>TABLE OF CONTENTS</b>		
I. INTRODUCTION	1	
II. BACKGROUND	2	
III. DISCUSSION	10	
A. Defining "Breach"	12	
B. Notifying the Commission and other Federal Law Enforcement of Data Breaches	23	
C. Customer Notification	31	
D. TRS Breach Reporting	42	
E. Legal Authority	46	
F. Impact of the Congressional Disapproval of the 2016 Privacy Order	51	
G. Digital Equity Considerations	53	
IV. PROCEDURAL MATTERS	54	
V. ORDERING CLAUSES	60	
APPENDIX A – PROPOSED RULES		
APPENDIX B – INITIAL REGULATORY FLEXIBILITY ANALYSIS		
<b>I. INTRODUCTION</b>		
<p>I. The Commission first adopted a rule in 2007 requiring telecommunications carriers and interconnected Voice over Internet Protocol (VoIP) providers to notify customers and federal law enforcement of breaches of customer proprietary network information (CPNI) in the carriers' possession.<sup>1</sup> In the almost decade and a half since that time, data breaches nationwide have increased in both frequency and severity.<sup>2</sup> In the telecommunications industry, the public has suffered an</p>		
<p><sup>1</sup> See <i>Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking</i>, 22 FCC Rcd 6927 (2007) (2007 CPNI Order), 47 CFR § 64.2011.</p> <p><sup>2</sup> Identity Theft Resource Center, <i>Identity Theft Resource Center to Share Latest Data Breach Analysis With U.S. Senate Commerce Committee: Number of Data Breaches in 2021 Surpasses All of 2020</i> (Oct. 6, 2021), <a href="https://www.itrcenter.org/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/">https://www.itrcenter.org/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/</a>; see also IAPP, <i>U.S. State Data Breach List</i>, <a href="https://iapp.org/resources/article/u-s-state-data-breach-list/">https://iapp.org/resources/article/u-s-state-data-breach-list/</a> (last visited Jan. 4, 2023) (compilation of the numerous states agency-maintained databases listing breaches reported in their states).</p>		

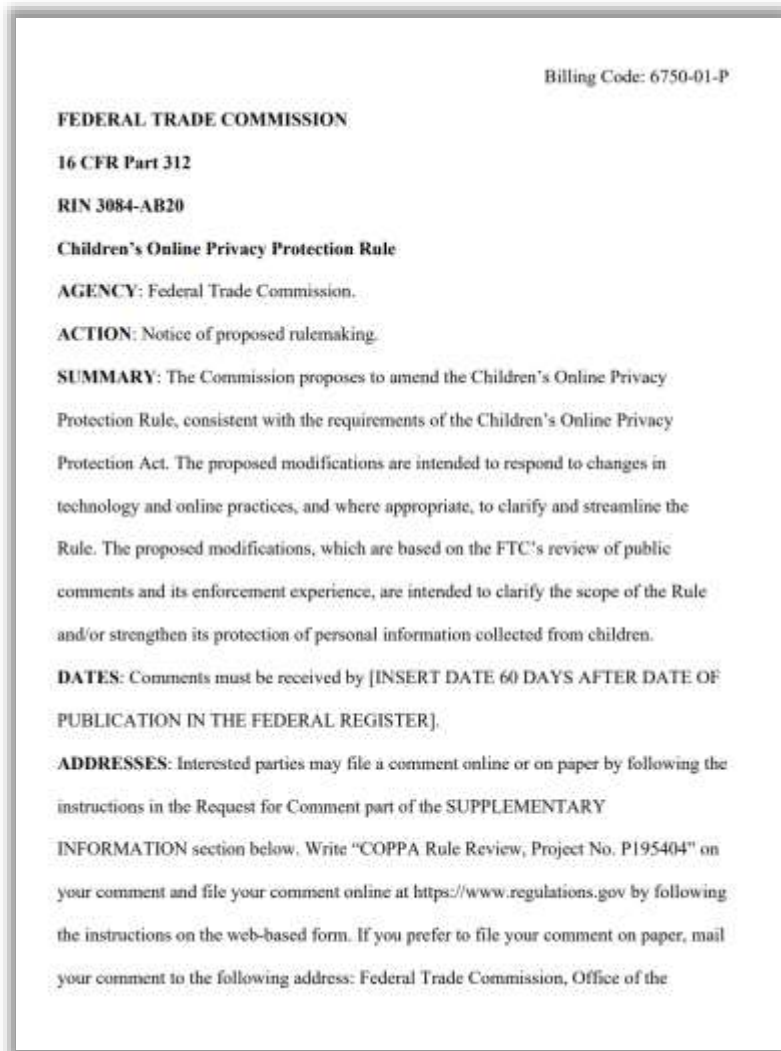
Федеральная комиссия по связи США (Federal Communications Commission, FCC) предложила обязать интернет-провайдеров и операторов связи информировать о любых утечках конфиденциальных данных потребителей и федеральные правоохранительные структуры «незамедлительно».

Согласно действующим нормам FCC от 2007 года, операторы, количество клиентов которых превышает пять тысяч, должны извещать правоохранительные агентства об утечках персональных данных в течение семи дней. Компании с меньшим количеством абонентов — в течение 30 дней.

Теперь об утечке данных операторы должны будут уведомлять абонентов, FCC, ФБР и Секретную службу (United States Secret Service) сразу же после выявления подобного факта, если иное не предусмотрено федеральными властями.

FCC также предложила расширить определение «утечки», включив в него неумышленный несанкционированный доступ к клиентской информации, а также её использование и раскрытие. Сейчас регулятор считает утечкой получение внешним агентом несанкционированного доступа к конфиденциальной информации.

## FTC в США предложила ввести новые ограничения на сбор технологическими компаниями данных детей



Федеральная торговая комиссия США (Federal Trade Commission, FTC) 20.12.2023 предложила внести новые нормы в рамках закона о защите конфиденциальности детей в Интернете (COPPA) для ограничения сбора и использования персональных данных (ПД) несовершеннолетних IT-фирмами, в частности, для ведения таргетированных рекламных кампаний.

◇ Так, технологические компании не должны будут предоставлять детям младше 13 лет возможность получать таргетированные рекламные сообщения по умолчанию. Для передачи ПД несовершеннолетних сторонним организациям IT-компаниям потребуется «отдельное верифицируемое родительское согласие».

◇ Предлагается запретить организациям прекращать предоставлять услуги несовершеннолетним в случае отказа детей от передачи данных для адресной рекламы.

◇ FTC помимо прочего намерена запретить технологическим компаниям использовать определённую информацию для отправки push-сообщений несовершеннолетним с призывом запустить то или иное приложение.

◇ Кроме того, ПД детей нельзя будет хранить неопределённо долго, сбор ПД образовательными компаниями предложено вести при согласии учебных заведений, а коммерческое использование подобных ПД — запретить.

<https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens>

<https://d-russia.ru/reguljator-v-ssha-predlozhil-vvesti-novye-ogranichenija-na-sbor-tehnologicheskimi-kompanijami-pd-detej.html>



The screenshot shows a news article from NextGov/FCW. The main headline is "Bipartisan bill protects artists' and individuals' likenesses from AI duplication". Below the headline is a photograph of a person performing on stage. The article text mentions that the popular recording artist The Weeknd was cited in a new bill that would protect artists' likenesses and work from unauthorized AI duplication. A sub-headline reads: "The No AI FRAUD Act penalizes cyber actors who leverage generative artificial intelligence and machine learning to duplicate images and voices without a person's consent." The article is dated January 10, 2024, and is written by Alexandra Kelley, Staff Correspondent at NextGov/FCW. A "CONGRESS" tag is visible. Social media sharing icons for X, LinkedIn, Facebook, and Email are present. A short summary at the bottom states: "Lawmakers are continuing to try to fill the legal gaps accompanying rapid innovations in artificial intelligence technologies with a new bill introduced Wednesday that targets fake content generated by machine learning models."

Проект предполагает наказание за применение искусственного интеллекта (ИИ) для генерации фото- видеоизображений, а также имитации голосов людей.

Закон дает право собственности физическим лицам на свой голос и внешность. Их передача может осуществляться исключительно самим человеком. Также авторское право продолжает действовать даже после смерти физического лица.

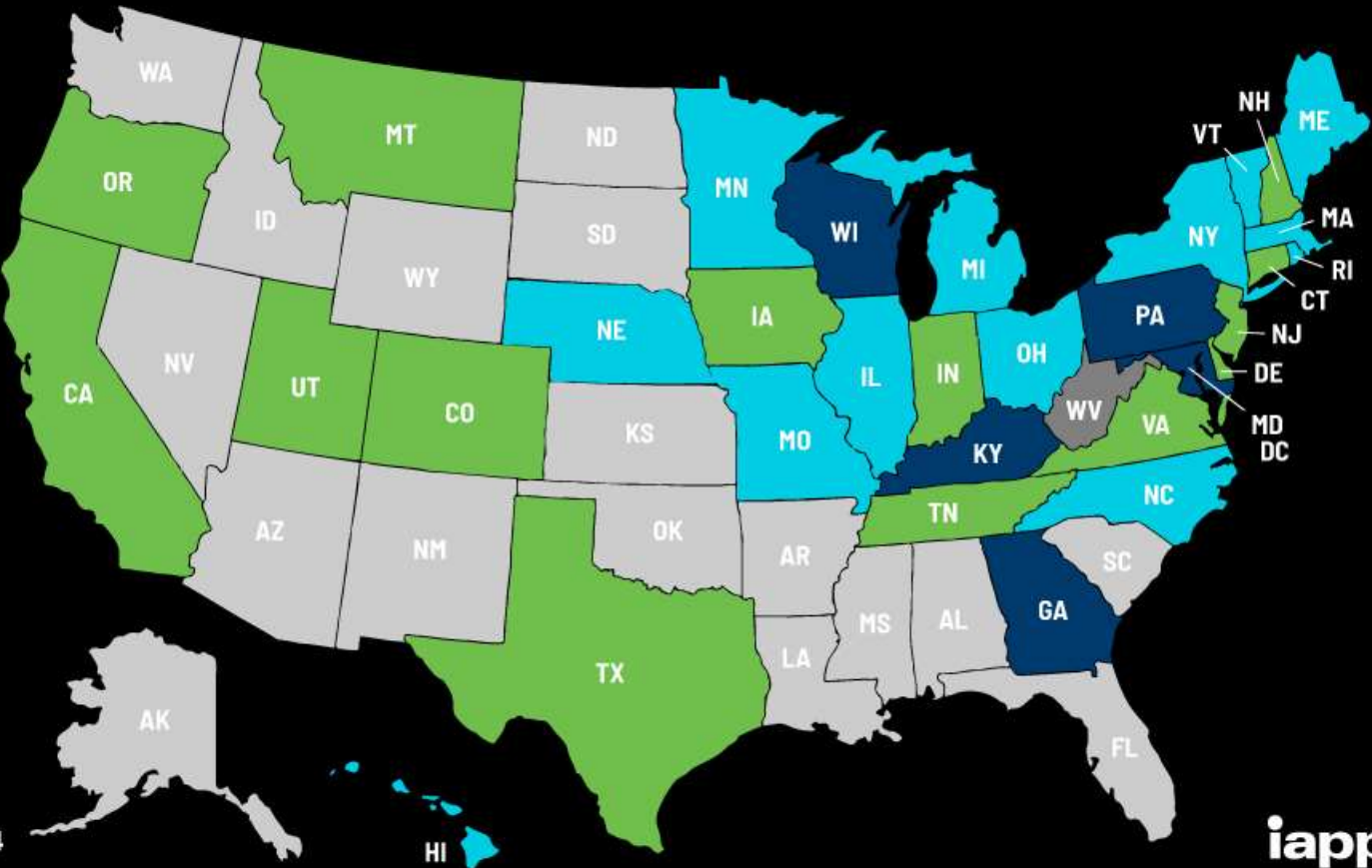
Предполагаемый штраф за незаконное копирование и фальсификацию до 50 тыс. долларов.

Данный законопроект связан с последними скандалами в медиаиндустрии. Например, в ноябре 2023 года американская актриса Скарлетт Йоханссон подала в суд за незаконное использование своей внешности в ролике. Также это коснулось имитации голоса известных американских исполнителей, таких как Дрейк и The Weeknd.

# US State Privacy Legislation Tracker 2024

Statute/bill in legislative process

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced



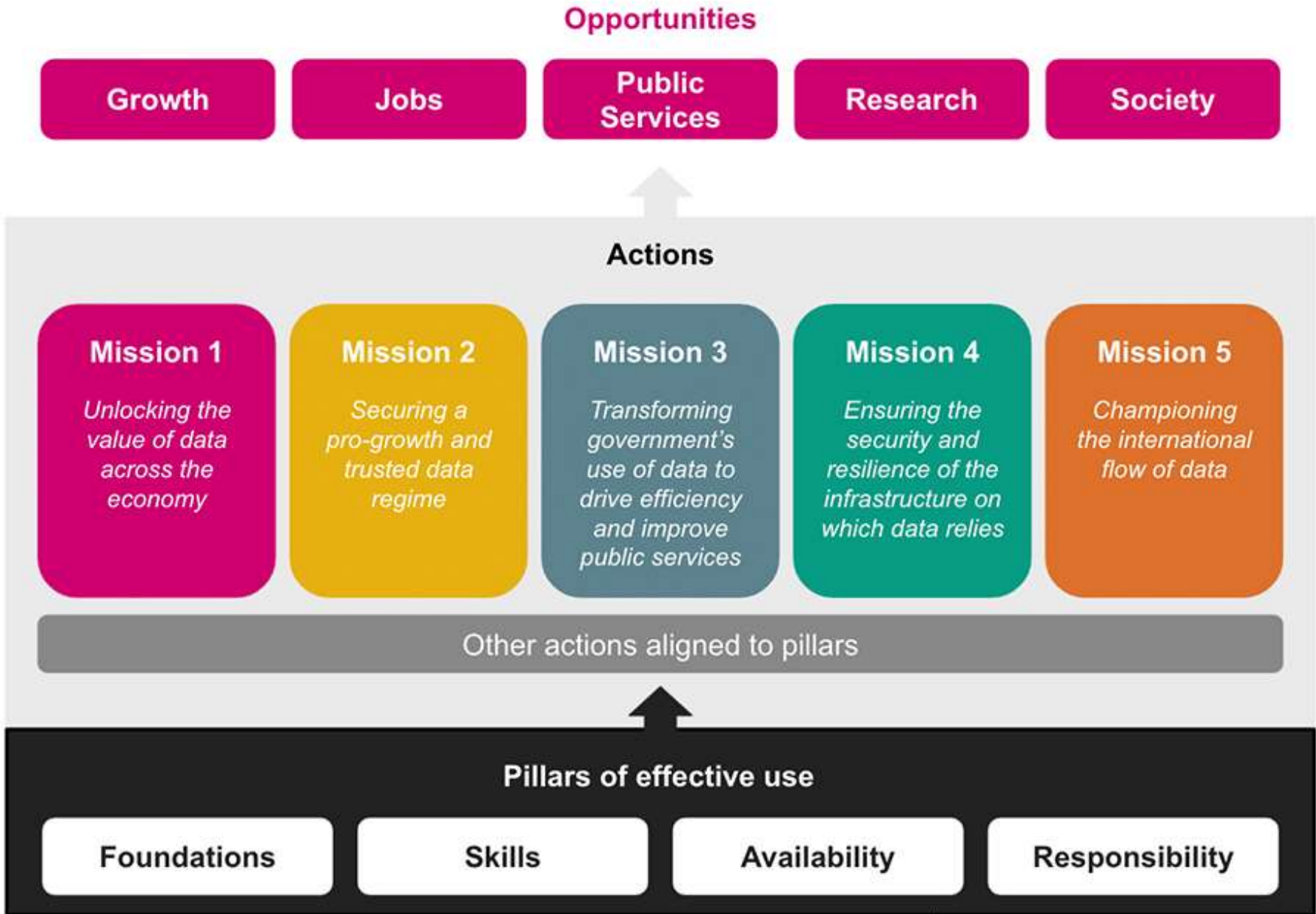
Last updated 22 March 2024



## Эра пост-GDPR в Великобритании





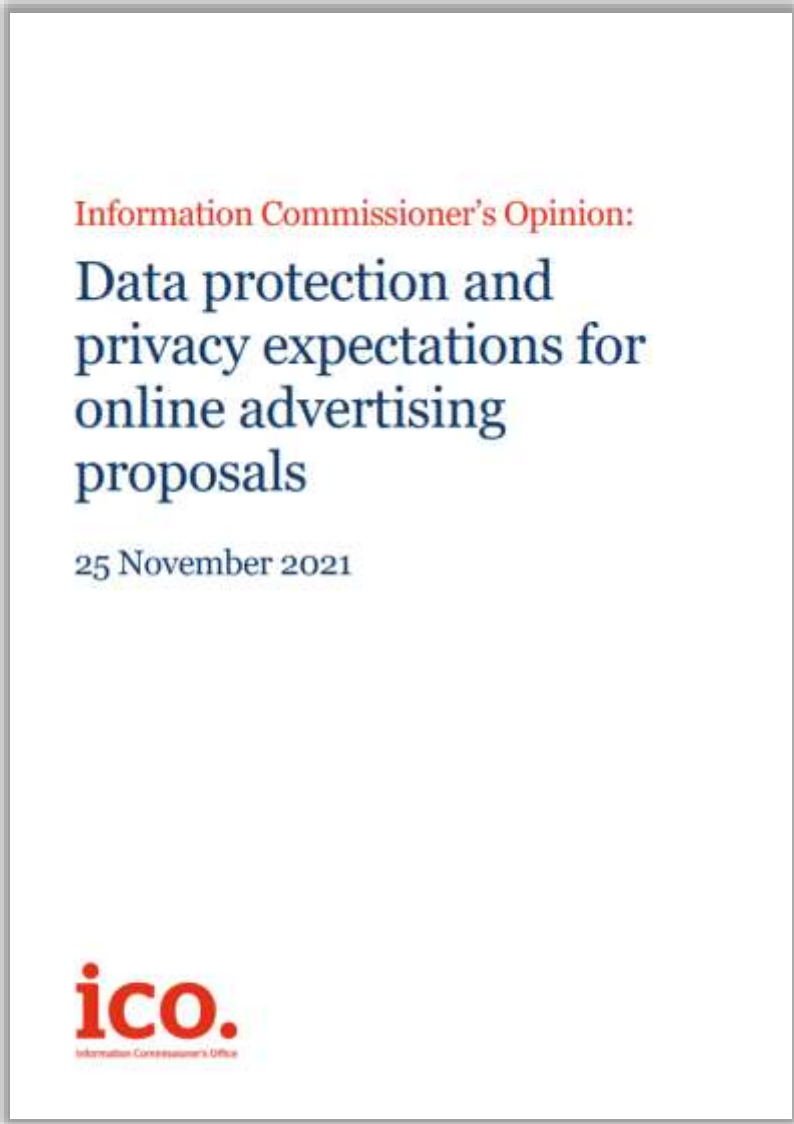


## Руководство об обработке персональных данных в Великобритании и обмене данными с ЕС после Brexit

The screenshot shows the GOV.UK website interface. At the top, there is a search bar and navigation links for 'Departments', 'Worldwide', 'How government works', and 'Get involved'. Below the search bar, there are links for 'Coronavirus (COVID-19)' and 'The UK and EU transition'. The main content area features a breadcrumb trail: 'Home > Business and industry > Business regulation > Sale of goods and services and data protection'. A section titled 'Part of Transition period' is visible. The main heading is 'Guidance Using personal data in your business or other organisation after the transition period'. Below this, a sub-heading reads: 'What action you need to take regarding data protection and data flows with the EU/EEA after the end of the transition period.' The page is dated 'Published 16 October 2020' and lists the authors: 'Department for Digital, Culture, Media & Sport, Department for Business, Energy & Industrial Strategy, Office for Civil Society, and Information Commissioner's Office'. A black box at the bottom contains the text: 'New rules for January 2021. The UK has left the EU, and the transition period after Brexit comes to an end this year. This page tells you what you'll need to do from 1 January 2021. It will be updated if anything changes. Check what else you need to do during the transition period.'

Ряд уполномоченных органов Великобритании (Department for Digital, Culture, Media & Sport, Department for Business, Energy & Industrial Strategy, Office for Civil Society и Information Commissioner's Office) 16.10.2020 выпустили совместное руководство для британского бизнеса в отношении обработки персональных данных и трансграничного обмена данными с ЕС/ЕЭЗ после окончания переходного периода Brexit.

# Мнение ICO в отношении защиты данных и приватности для онлайн-рекламы



- 1. Executive summary .....3
- 2. Introduction.....5
  - 2.1 The Commissioner’s work on adtech .....6
  - 2.2 Recent market developments .....7
  - 2.3 Purpose of this Opinion .....8
  - 2.4 Scope of this Opinion.....9
- 3. Online advertising developments..... 12
  - 3.1 The meaning of “online tracking” ..... 13
  - 3.2 Key issues highlighted in the 2019 report ..... 16
  - 3.3 Removal of third-party cookies ..... 19
  - 3.4 Browser and software developments .....20
  - 3.5 The Google Privacy Sandbox .....22
  - 3.6 Developments related to user preferences and identifiers ..... 25
  - 3.7 Standards body processes.....29
  - 3.8 The Commissioner’s work with the CMA.....30
- 4. Data protection concerns .....32
  - 4.1 First parties and third parties.....33
  - 4.2 Purpose limitation .....37
  - 4.3 Internal disclosure and external data sharing .....39
  - 4.4 “Privacy as a shield” ..... 41
- 5. The Commissioner’s expectations .....43
  - 5.1 Principles .....43
  - 5.2 Recommendations .....44
- 6. Conclusions and next steps .....47

## ICO призывает правительство пересмотреть использование частной электронной почты и приложений для обмена сообщениями



Управление комиссара по информации (ICO) опубликовало 11.07.2022 отчет под названием «За экранами - поддержание прозрачности правительства и безопасности данных в эпоху приложений для обмена сообщениями».

в отчете подробно описывается расследование ICO по использованию коммерческих сервисов электронной почты, WhatsApp и других мессенджеров министрами и чиновниками Министерства здравоохранения и социального обеспечения (DHSC) во время пандемии. В частности, в ходе расследования было установлено, что существовали реальные риски для прозрачности и подотчетности, отсутствие надлежащего организационного или технического контроля для обеспечения эффективной безопасности и управления рисками использования таких каналов коммуникации.

Соответственно, ICO вынесло DHSC выговор за нарушение статей 5(1)(e), 5(1)(f), 25 и 32 Общего положения о защите данных Великобритании ("UK GDPR"), которое требует от DHSC, помимо прочего, улучшить свои процессы и процедуры обработки персональных данных посредством мессенджеров и коммерческих сервисов электронной почты.

# International data transfer agreement (IDTA) о дополнении к EU SCC с 21.03.2022

**SCHEDULE 1  
(AS REFERENCED IN EXPLANATORY MEMORANDUM)**



Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

---

**International Data Transfer Agreement**

**VERSION A1.0, in force 21 March 2022**

---

This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

**Part 1: Tables**

**Table 1: Parties and signatures**

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
<b>Parties' details</b>	Full legal name: <input type="text"/> Trading name (if different): <input type="text"/> Main address (if a company registered address): <input type="text"/> Official registration number (if any) (company number or similar identifier): <input type="text"/>	Full legal name: <input type="text"/> Trading name (if different): <input type="text"/> Main address (if a company registered address): <input type="text"/> Official registration number (if any) (company number or similar identifier): <input type="text"/>
<b>Key Contact</b>	Full Name (optional): <input type="text"/> Job Title: <input type="text"/>	Full Name (optional): <input type="text"/> Job Title: <input type="text"/>

**SCHEDULE 3  
(AS REFERENCED IN EXPLANATORY MEMORANDUM)**



Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

---

**International Data Transfer Agreements – Transitional Provisions**

**In force 21 March 2022**

---

**Background:**

Chapter V of the "UK GDPR" (as defined in Section 3(10) of the Data Protection Act 2018 ("DPA")) governs international transfers of personal data by controllers and processors ("data exporters").

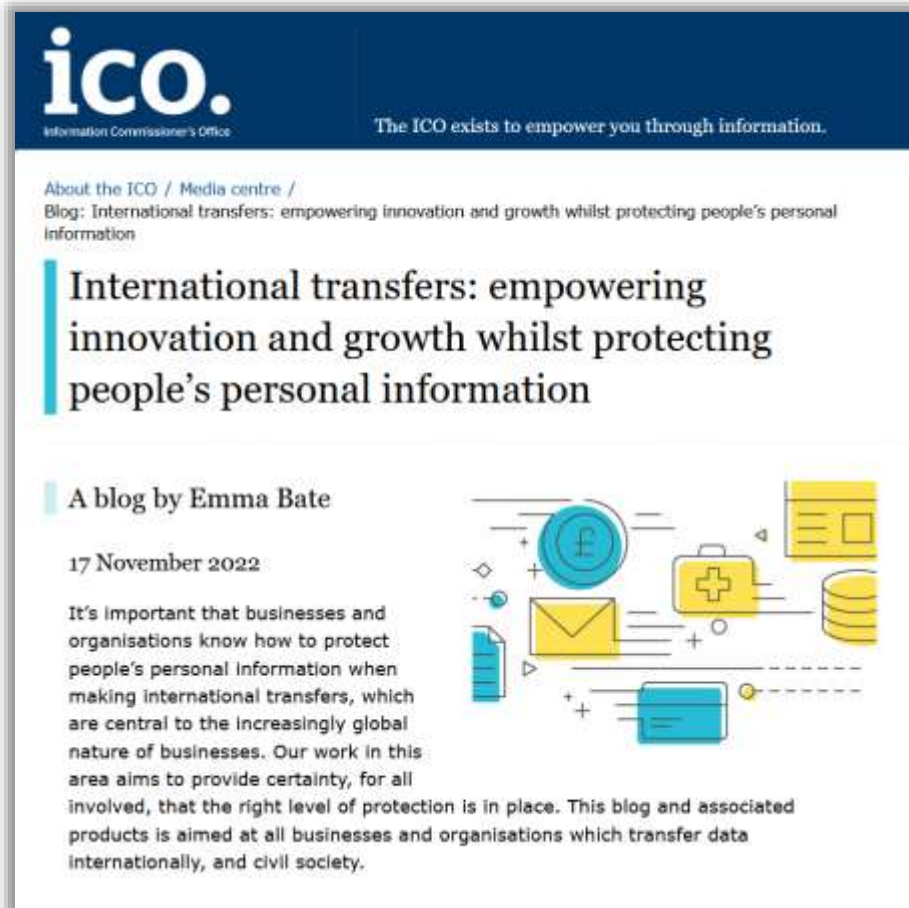
Article 46(1) of the UK GDPR allows international transfers of data where the data exporter has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Paragraph 7 of Part 3 in Schedule 21 of the DPA sets out transitional provisions allowing the continued use by data exporters of standard data protection clauses which were issued under the Data Protection Directive 95/46/EC, as an appropriate safeguard under Article 46(1) of the UK GDPR. In particular, the standard data protection clauses which were issued under European Commission Decision 2001/497/EC and European Commission Decision 2010/87/EU.

In this document, "Transitional Standard Clauses" means those standard data protection clauses which by virtue of Paragraph 7 of Part 3 in Schedule 21 of the DPA provide the appropriate safeguards referred to in Article 46(1) of the UK GDPR.

Paragraph 8 of Part 3 in Schedule 21 of the DPA allows the Information Commissioner to disapply Paragraph 7, and so the use of the Transitional Standard Clauses as appropriate safeguards under Article 46(1) of the UK GDPR.

## 1190 Развитие регулирования международной передачи данных в Великобритании



The image shows a screenshot of a blog post from the Information Commissioner's Office (ICO). The header features the ICO logo and the tagline "The ICO exists to empower you through information." Below the header, there is a navigation menu with "About the ICO / Media centre /" and "Blog: International transfers: empowering innovation and growth whilst protecting people's personal information". The main title of the blog post is "International transfers: empowering innovation and growth whilst protecting people's personal information". The author is identified as "A blog by Emma Bate" and the date is "17 November 2022". The text of the blog post discusses the importance of protecting personal information in international transfers and mentions a "TRA Tool" with six questions and tables for use in work.

**ico.**  
Information Commissioner's Office

The ICO exists to empower you through information.


About the ICO / Media centre /  
Blog: International transfers: empowering innovation and growth whilst protecting people's personal information

### International transfers: empowering innovation and growth whilst protecting people's personal information

A blog by Emma Bate

17 November 2022

It's important that businesses and organisations know how to protect people's personal information when making international transfers, which are central to the increasingly global nature of businesses. Our work in this area aims to provide certainty, for all involved, that the right level of protection is in place. This blog and associated products is aimed at all businesses and organisations which transfer data internationally, and civil society.



Управление комиссара по информации (Information Commissioner's Office) Великобритании опубликовало дополнение к руководству по международной передаче данных. Появился новый раздел об оценке рисков передачи (Transfer Risk Assessments, TRA).

Раздел об оценке рисков разъясняет альтернативный подход по сравнению с подходом, предложенным Европейским советом по защите данных. Дополнительно представлен TRA Tool из шести вопросов с руководством и таблицами для использования в работе.

## 1191 Руководство ICO по TRA при передаче данных в США



The screenshot shows the ICO website header with the logo and tagline 'The ICO exists to empower you through information.' Below the header is a navigation menu with links: Home, For the public, For organisations, Make a complaint, and Action we've taken. The main content area has a breadcrumb trail: For organisations / UK GDPR guidance and resources / International transfers / International data transfer agreement and guidance / International data transfer agreement and guidance / Transferring personal information to the US. The main heading is 'Completing a transfer risk assessment when transferring personal information to the US using an Article 46 transfer mechanism'. Below this, there are sections for 'Who is this guidance for?' and 'At a glance'. The 'Who is this guidance for?' section states that the guidance is relevant for restricted transfers of personal information to the US using an Article 46 transfer mechanism, with examples like IDTA, Addendum to the EU SCCs, and BCRs. The 'At a glance' section notes that restricted transfers to the US require a completed TRA and encourages reliance on the DSIT's published analysis to streamline the process.

**ico.**  
Information Commissioner's Office

The ICO exists to empower you through information.

Home For the public For organisations Make a complaint Action we've taken

For organisations / UK GDPR guidance and resources / International transfers /  
International data transfer agreement and guidance /  
International data transfer agreement and guidance / Transferring personal information to the US

### Completing a transfer risk assessment when transferring personal information to the US using an Article 46 transfer mechanism

#### Who is this guidance for?

This guidance is relevant to you if you wish to make a restricted transfer of personal information to a recipient in the US using an Article 46 transfer mechanism. These are the "appropriate safeguards" listed in Article 46 of the UK GDPR. Examples are the ICO's International Data Transfer Agreement (IDTA), the Addendum to the EU SCCs (the Addendum) and Binding Corporate Rules (BCRs).

#### At a glance

You may only make restricted transfers of personal information to recipients in the US using an Article 46 transfer mechanism if you have first completed a transfer risk assessment (TRA).

We encourage you to rely on the Department for Science, Innovation and Technology (DSIT)'s published analysis to streamline your TRA process for US transfers. The DSIT analysis considers US laws related to access and use of personal information by US agencies for the purposes of national security and law enforcement. This guidance explains how you can use that analysis as part of your TRA process for US transfers.

Управление комиссара по информации (Information Commissioner's Office) Великобритании 15.12.2023 опубликовало руководство по оценке рисков передачи (TRA) при передаче персональных данных в США с использованием механизма передачи, предусмотренного ст.46 UK GDPR. Руководство призвано помочь организациям, желающим осуществить ограниченную передачу персональных данных в США с использованием специальных механизмов передачи.

В руководстве подчеркивается, что после рассмотрения дела Schrems II в 2020 году перед передачей персональных данных за пределы Великобритании с использованием механизма передачи, предусмотренного ст.46 UK GDPR, необходимо провести TRA. Руководство поощряет использование анализа Министерства науки, инноваций и технологий (DSIT) для упрощения процесса TRA для передачи данных за пределы США. В анализе DSIT оцениваются законы США, связанные с доступом и использованием личной информации в целях национальной безопасности и правоохранительных органов.

## 1192 UK-US Data Bridge

Министерство науки, инноваций и технологий (Department of Science, Innovation and Technology, DSIT) опубликовало Правила защиты данных (адекватности) для передачи данных в США (Data Protection (Adequacy) (USA) Regulations 2023) в качестве Британского дополнения (UK-US Data Bridge) к EU-US Data Privacy Framework (EU-US DPF), которые вступают в силу 12.10.2023. Государственный секретарь Соединенного королевства определил США в качестве страны, обеспечивающей адекватный уровень защиты персональных данных при передаче данных, отвечающих следующим критериям:

- трансграничная передача данных осуществляется лицу в США, включенному в список участников UK-US Data Bridge;
- последующая обработка переданных данных будет подпадать под действие принципов EU-US DPF.

Независимыми надзорными органами в рамках UK-US Data Bridge являются Федеральная торговая комиссия США (FTC) и Министерство транспорта США (DoT), находящееся в ведении Министерства торговли (DoC).

Примечательно, что британские организации не могут свободно передавать персональные данные любому американскому импортеру/получателю данных. Для облегчения передачи данных получатель должен быть сертифицирован в соответствии с UK-US Data Bridge и включен в соответствующий [список](#). В настоящее время право на участие в программе DPF имеют только американские организации, находящиеся под юрисдикцией FTC или DoT. Другие американские организации, например, банковские, страховые и телекоммуникационные, в настоящее время не могут участвовать в программе. Кроме того, данные, определяемые как журналистские не могут быть переданы в США в рамках UK-US Data Bridge.



## 1193 Британский ICO выразил сомнения относительно UK-US Data Bridge

- 1. Недостаточная защита чувствительных данных:** Определение «чувствительных данных» в мосте отличается от определения в британском GDPR. В DPF не указаны все специальные категории персональных данных, определенные в GDPR, такие как биометрические, генетические данные, данные о сексуальной ориентации и данные об уголовных преступлениях. Это может привести к тому, что указанные категории данных не будут должным образом защищены при передаче в США.
- 2. Отсутствие адекватной защиты данных об уголовных преступлениях:** В США отсутствует защита, сравнимая с защитой в Великобритании о реабилитации правонарушителей 1974 года, который ограничивает использование данных об уголовных судимостях после погашения этих судимостей. Непонятно, как эти защиты будут применяться к информации, переданной в США.
- 3. Уменьшение прав на конфиденциальность:** В мосте отсутствует существенно схожее с британским GDPR право на защиту от принятия решений на основе исключительно автоматизированной обработки, которые могут иметь юридические или аналогичные последствия для субъекта данных. Также отсутствует аналогичное «право быть забытым» или возможность отозвать согласие, что ограничивает контроль субъектов данных над их персональной информацией.
- 4. Недостаточные гарантии для защиты прав субъектов данных в случае принятия решений на основе автоматизированной обработки:** В Data Bridge не предусмотрено право на пересмотр автоматизированного решения человеком, что может привести к нарушению прав субъектов данных в случае принятия решений, основанных исключительно на автоматизированной обработке.
- 5. Недостаточный контроль над персональными данными:** Права, предоставляемые мостом, не такие обширные, как права, предоставляемые британским GDPR, что может уменьшить контроль субъектов данных над их личной информацией, особенно в отношении отзыва согласия и права быть забытым.
- 6. Специфические требования для передач данных из Великобритании:** Компании, которые не могут использовать мост данных, могут столкнуться с необходимостью полагаться на другие механизмы, такие как SCCs или BCRs. Это может потребовать дополнительных усилий и ресурсов для обеспечения соблюдения требований британского GDPR.
- 7. Изменения в использовании Стандартных контрактных условий (SCC):** Экспортеры данных из Великобритании должны быть осведомлены о том, что SCC EC больше не могут использоваться для новых соглашений о передаче данных из Великобритании. Требуется либо дополнение к SCC EC, либо использование Международного соглашения о передаче данных (International Data Transfer Agreement, IDTA), что может создать дополнительные проблемы и потребовать дополнительных ресурсов.

# 1194 Data Protection and Digital Information Bill vs GDPR

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill
<p><b>Privacy and Electronic Communications Directive 2002 as amended by Directive 2009/136/EC of the (ePrivacy Directive)</b></p> <p><b>Article 15a (Duty to notify the Commissioner of unlawful direct marketing)</b> The powers of supervision and enforcement are delegated to member states to determine and therefore not specified at an EU level.</p>	<p><b>Clause 85 (Duty to notify the Commissioner of unlawful direct marketing)</b> The DPDI Bill introduces a duty on providers of public electronic communication services and networks to report to the Information Commissioner suspicious activity relating to unlawful direct marketing. As a consequence, a new power is introduced for the Information Commissioner to issue fines of up to 1,000 pounds to service providers and network providers who violate the regulation.</p>
<p><b>Article 15a (Enforcement powers)</b> The powers of supervision and enforcement are delegated to member states to determine and therefore not specified at an EU level.</p>	<p><b>Clause 86 (Enforcement powers)</b> The current UK enforcement powers under the Privacy and Electronic Communications Regulations have been expanded to broadly reflect those available under the UK GDPR. This includes making cookies and electronic direct marketing infringements subject to increased fines of up to 20 million euros or 4% of annual worldwide turnover, whichever is higher, compared with a maximum of 500,000 pounds previously.</p>

In conclusion, the Data Protection and Digital Information Bill covers a significant number of important provisions within the current EU GDPR framework. However, none of the proposed changes represent a radical departure from the current law. In fact, the UK government has sought to simplify compliance, but not to eliminate the basic rules of UK data protection law. From a perspective, the essential similarities between the two regimes will not cease to exist once the DPDI Bill is enacted.

The UK Data Protection and Digital Information Bill • International Association of Privacy Professionals • iapp.org

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill
<p><b>Definitions</b></p> <p><b>Article 4 and Recital 33 (Consent for scientific research)</b> The EU GDPR requires that where consent is relied on as the lawful basis for processing, the consent must be given for a specific purpose or purposes. The text raises challenges in the context of exploratory scientific research, where it may not be possible to fully identify the objective of the research at the outset. The main body of the EU GDPR does not provide a solution to this, although recital 33 notes that individuals should be allowed to consent to areas of research where in keeping with recognized ethical standards, and when individuals are given the option of consenting only to part of the research where practical.</p>	<p><b>Clause 3 (Consent for scientific research)</b> The DPDI Bill moves the substance of the recital into the body of the UK GDPR but does not substantively alter its meaning.</p>
<p><b>Principles and lawful grounds of processing</b></p> <p><b>Article 6(1) and (f) (Lawfulness of processing)</b> The EU GDPR requires that all processing has a lawful ground. One of these lawful grounds is that the processing is necessary for the purposes of the legitimate interests of the controller or a third party, and those interests are not overridden by the interests or fundamental rights of the data subject. Relying on this lawful ground requires conducting a balancing test on a case-by-case basis. An alternative legal basis is where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.</p>	<p><b>Clause 5 and Schedule 1, Annex 1 (Lawfulness of processing)</b> The DPDI Bill removes the need to assess whether processing for certain "recognized" legitimate interests is overridden by the interests or rights of the data subject. These "recognized" legitimate interests are laid out in Annex 1. A procedure is set out for the UK government to add to the list in the future. The current list focuses on "public interests" such as national security, public security, defense, emergencies, preventing crime, safeguarding and democratic engagement.</p>

The UK Data Protection and Digital Information Bill • International Association of Privacy Professionals • iapp.org

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
<p><b>Article 12 and Article 15-22 (Objections or excessive requests and time limits for responding)</b> The EU GDPR provides data subjects with certain rights exercisable against controllers, including the right of access, right to modification, right to erasure, the right to restrict processing, right to data portability and right to object. Requests cannot be refused unless the controller can demonstrate it is not in a position to identify the data subject or if the request is manifestly unfounded or excessive. The EU GDPR states that this may be the case in particular because of their repetitive character but does not explicitly define these terms. Controllers have one month from receipt of the request to respond substantively, although this may be extended by two further months where necessary, taking into account the complexity and number of requests.</p>	<p><b>Clause 7 and Clause 8 (Objections or excessive requests and time limits for responding)</b> The DPDI Bill replaces the EU GDPR's "manifestly unfounded or excessive" threshold for refusing requests with a new "reasons or excessive" threshold. The DPDI Bill outlines several factors to be considered when determining whether requests meet this threshold, together with examples of requests which may do so. Among other things, controllers will now be able to take into account their resources and may be able to refuse requests intended to cause distress, not made in good faith, or which are an abuse of process. The DPDI Bill also clarifies that the time period for responding to a request does not run whilst waiting for a requestor to confirm their identity (if requested), provide any reasonably necessary clarifications requested by the controller, or to pay any fees due.</p>	<ul style="list-style-type: none"> <li>The UK approach expands the circumstances under which a request may be refused and provides helpful clarity that the clock does not continue to run whilst waiting for the requestor to provide any necessary information that is requested.</li> <li>Applying the EU interpretation in the UK will be complex.</li> <li>The UK approach makes it simpler to comply with individuals' rights.</li> </ul>
<p><b>Article 13 and Article 14 (Information to be provided to data subjects)</b> The EU GDPR requires controllers to provide certain transparency information to the data subject. There are certain exemptions to this requirement. In particular, where personal data has not been obtained directly from the data subject, it is not necessary to provide the information where it would (a) be impossible, (b) involve disproportionate effort, or (c) undermine the objectives of the processing. Instead, it is sufficient to take appropriate steps to protect the data subject, which must include making the information publicly available (for example via a privacy notice).</p>	<p><b>Clause 9 (Information to be provided to data subjects)</b> The DPDI Bill expands this exemption such that it also applies to processing personal data which has been collected directly from the data subject for research, archiving or statistical purposes only, where providing such information would be impossible or require disproportionate effort.</p>	<ul style="list-style-type: none"> <li>The UK approach makes it less onerous to comply with transparency obligations when processing personal data collected directly from the data subject for research, archiving or statistical purposes only.</li> <li>Applying the EU interpretation in the UK will be complex.</li> <li>The UK approach is simpler to comply with when processing personal data collected directly from the data subject for research, archiving or statistical purposes only.</li> </ul>

The UK Data Protection and Digital Information Bill • International Association of Privacy Professionals • iapp.org

<https://bills.parliament.uk/bills/3322>

<https://iapp.org/resources/article/uk-dpdi-bill-comparison-gdpr-eprivacy/>

# 1195 Data Protection and Digital Information (No.2) Bill

## Bill passage



<https://bills.parliament.uk/bills/3430>

<https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum>



The screenshot shows the ICO website header with the logo and tagline 'The ICO exists to empower you through information.' Below the header is a navigation menu with links: Home, For the public, For organisations, Make a complaint, and Action we've taken. The main content area features the article title 'Data breaches put domestic abuse victims' lives at risk, UK Information Commissioner warns' with a date of 27 September 2023 and a type of News. A list of bullet points provides details about the warning, including the number of organizations reprimanded and the nature of the data breaches. An image of a person's face with white paper cutouts covering their eyes and mouth is positioned to the right of the text.

**ico.**  
Information Commissioner's Office

The ICO exists to empower you through information.

Home For the public For organisations Make a complaint Action we've taken

About the ICO / Media centre / News and blogs /  
Data breaches put domestic abuse victims' lives at risk, UK Information Commissioner warns

### Data breaches put domestic abuse victims' lives at risk, UK Information Commissioner warns

Date: 27 September 2023  
Type: News

- Warning comes after the ICO reprimands seven organisations in the past 14 months for data breaches affecting victims of domestic abuse.
- Most cases related to organisations inappropriately disclosing the victim's home address to alleged perpetrators.
- Commissioner urges organisations to take responsibility for training their staff and putting appropriate systems in place to avoid such incidents.
- The action is supported by organisations including Women's Aid and the Domestic Abuse Commissioner for England and Wales



Служба информационного комиссара Великобритании (ICO), местный регулятор в области защиты личных данных, обратил внимание организаций, обрабатывающих личную идентифицирующую информацию граждан (PII), на опасность утечек персональных данных жертв домашнего насилия. Подобные нарушения могут ставить жизни людей под вполне реальную угрозу.

За последние 14 месяцев ICO вынесла выговоры семи организациям из-за нарушений в хранении конфиденциальной информации. Среди них оказались юридическая фирма, жилищная ассоциация, медицинский траст, государственный департамент, местные советы и полицейская служба. Среди выявленных случаев:

- ◇ Четыре ситуации, когда организации раскрывали безопасные адреса жертв обвиняемым. В одном случае пострадавшую семью пришлось немедленно переселять.

- ◇ Случайные раскрытия личности женщин, пытавшихся узнать информацию о своих партнёрах, этим партнёрам.

- ◇ Раскрытие домашнего адреса двух усыновлённых детей их родному отцу, отбывающему наказание за изнасилование их матери.

- ◇ Отправка неотредактированных отчётов с конфиденциальной информацией о детях в зоне риска, бывшим партнёрам их матери.

# Подборка ресурсов по GDPR



**Welcome to GDPRhub**

[Main page](#) [Discussion](#) [View source](#) [History](#)

**GDPRhub is a free and open wiki that allows anyone to find and share GDPR insights across Europe**

The content on GDPRhub is divided into two databases: decisions and knowledge.

In the **decisions** section we collect summaries of decisions by national DPAs and courts in English. The summaries can be searched by relevant GDPR article, issuing DPA or deciding court. Every day we monitor more than 50 webpages in each Member State. This page currently contains 100+ decisions and the goal is to reach 500+ by the end of 2020. We believe a good overview of national decisions is a key to a pan-European debate on the interpretation of contentious GDPR issues. Get all new decisions delivered right to your mailbox and subscribe to the [GDPRtoday newsletter!](#)

In the **knowledge** section we collect commentaries on GDPR articles, DPA profiles, and 32 GDPR jurisdictions (EU + EEA). In this database you can find anything from the phone number of the Icelandic DPA to a deep dive into each article of the GDPR.

Your [noyb.eu](#) Team

GDPR Decision Database			GDPR Knowledge		
Here you can find 100+ national GDPR decisions, arranged by GDPR Article, DPAs or the relevant Courts.			Here you can find a commentary on the first 21 GDPR Articles, profiles on 32 DPAs and profiles on 32 GDPR jurisdictions.		
Decisions by Articles	DPA Decisions	Court Decisions	GDPR Commentary	DPA Profiles	Jurisdiction Profiles

**Get a summary of new decisions with GDPRtoday!**

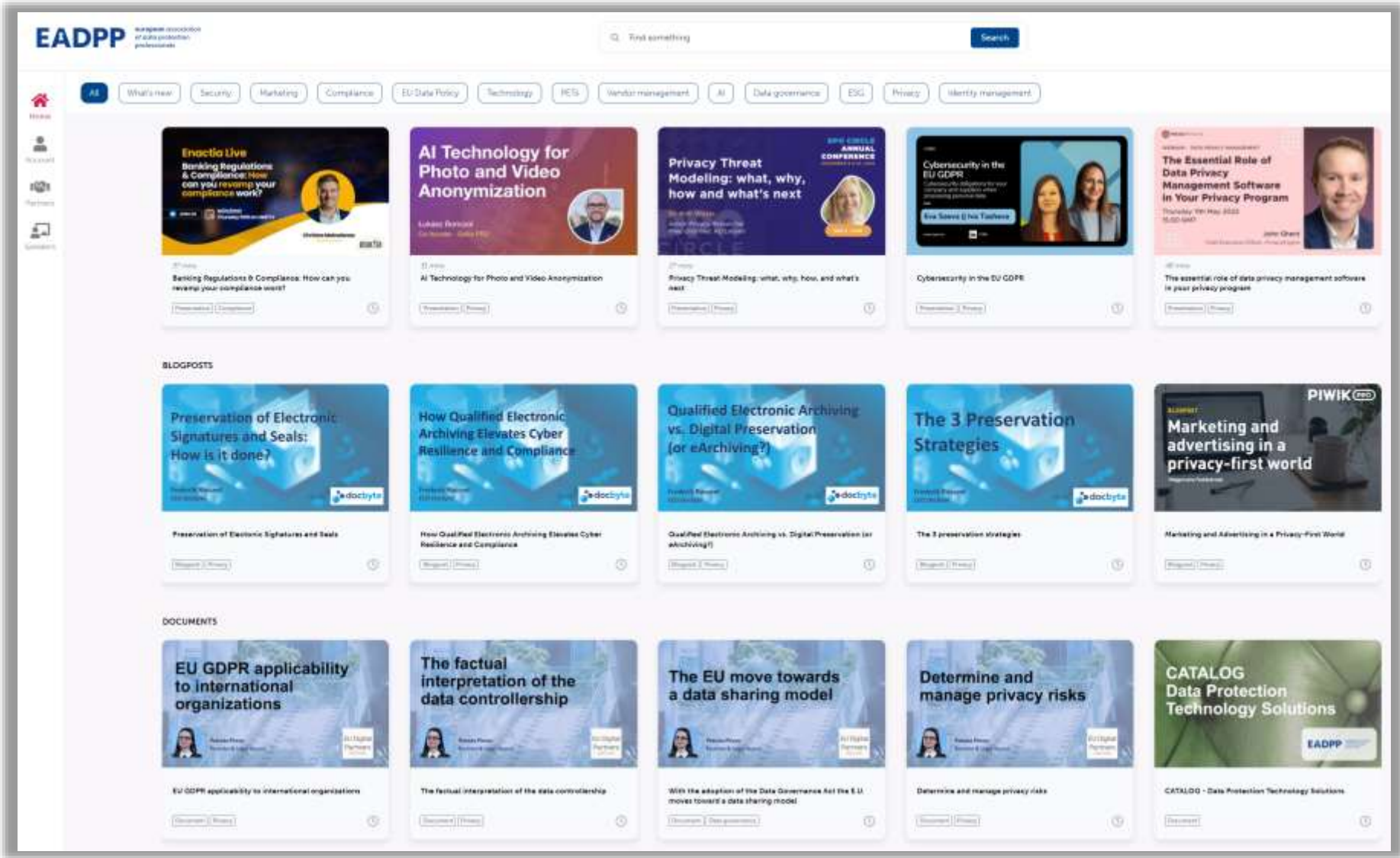
Our team will send you a quick overview of all national decisions of the past days from all across Europe - right to your mailbox and in English. Obviously it's free and you can cancel at any time!

[SUBSCRIBE NOW!](#)

**GDPRtoday**

НКО "None of Your Business" («Не твоё дело») по защите приватности, созданная широко известным в узких кругах Максом Шремсом, запустила новый ресурс для любителей европейского законодательства о защите данных, который предоставляет собой созданную на wiki-движке базу европейской правоприменительной и судебной практики GDPR. Эта база данных даёт представление о ключевых дискуссиях по интерпретации спорных вопросов GDPR. GDPRhub также содержит базу знаний о GDPR, которая содержит информацию о толковании и понимании отдельных положений европейского законодательства о защите данных.

# 1199 База документов, презентаций и публикаций EADPP



- <https://eadpp.insightz.io/category/10/Presentations>
- <https://eadpp.insightz.io/category/11/Documents>
- <https://eadpp.insightz.io/category/12/Blogposts>

## 1200 Лучшие блоги и новостные сайты о GDPR

1	 <a href="#">GDPR.Report</a>	353	15	0	613.8K	44	13/week	United Kingdom
2	 <a href="#">Act Now Training Blog</a>	0	24	0	0	32	1/day	United Kingdom
3	 <a href="#">Data Protection – IT Governance Blog</a>	2.6K	19.9K	0	135.9K	58	1/month	United Kingdom
4	 <a href="#">Privacy Matters - DLA Piper Blogs</a>	12.1K	39.4K	6.7K	101K	66	2/day	Chicago, Illin...
5	 <a href="#">Erwin   The Data Governance Company</a>	978	3.7K	0	272K	48	1/week	Melville, New...
6	 <a href="#">GetComplied Blog</a>	152	1.5K	637	0	14	16/year	Lisbon, Portu...
7	 <a href="#">OneSpan Data Security Blog</a>	10.7K	14	0	0	61	2/year	Chicago, Illin...
8	 <a href="#">Enlighten Blog</a>	6.4K	11.3K	0	391.4K	58	1/day	California, Un...
9	 <a href="#">General Data Protection Regulation - Reddit</a>	1.5M	674.7K	466K	18	91	3/day	San Francisc...
10	 <a href="#">Privacy International</a>	8.1K	63.1K	0	297.5K	72	1/day	London, Engl...
11	 <a href="#">Privacy Law Blog - Proskauer Rose</a>	488	356	798	327.7K	62	1/quarter	United States
12	 <a href="#">Fieldfisher - Privacy, Security and Information Law</a>	0	5.1K	403	687.1K	55	7/year	Netherlands
13	 <a href="#">Seers co Blog</a>	221	122	0	431K	34	3/week	London, Engl...
14	 <a href="#">easyGDPR</a>	0	13	0	0	16	2/month	Vienna, Austria
15	 <a href="#">White Label Consultancy</a>	0	0	0	8.9M	4	2/month	Oslo, Norway
16	 <a href="#">GDPR Ireland - GDPR.ie   Our Vision Your Data</a>	0	886	0	0	21	1/week	Dublin, Ireland
17	 <a href="#">EU Business Partners   Article 27 GDPR Representative</a>	5.3K	51	0	0	18	1/quarter	Cork, Ireland
18	 <a href="#">Relentless Data Privacy and Compliance</a>	13	54	124	0	17	30/year	Birmingham, ...
19	 <a href="#">dataprivacyfines.com</a>	0	0	0	0	3	30/year	
20	 <a href="#">GDPR Toolkit Blog - Supportica Group</a>	30	1.1K	0	4.8M	14		United Kingdom
21	 <a href="#">Trunomi Blog – Trunomi</a>	346	1K	0	920.9K	38	1/week	London, Engl...
22	 <a href="#">Signatu Blog - Georg Philip Krog</a>	0	45	0	0	22		Oslo, Norway



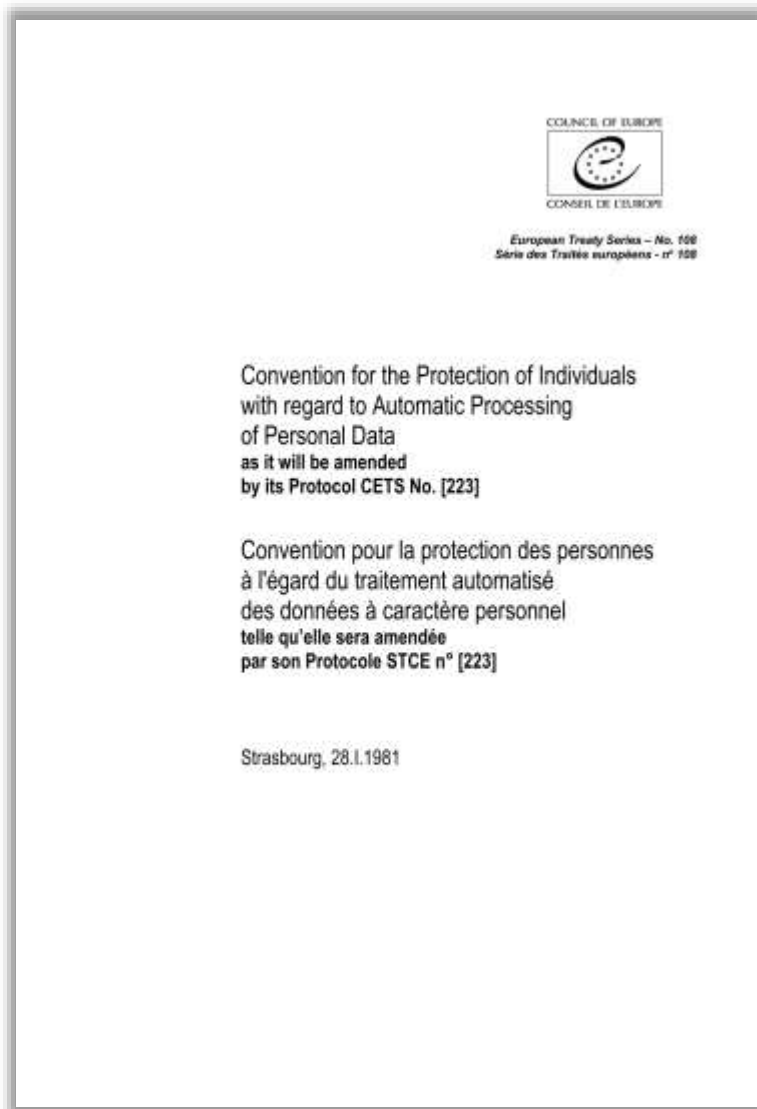
## 1201 Руководства по учету требований GDPR при разработке ПО

- Для веб-разработчиков: [руководство по приватности для браузеров](#) от команды разработчиков Chrome
- Для разработчиков приложений: [руководство по защите конфиденциальности пользователей](#), составленное Atlassian для разработчиков приложений, в котором описаны требования GDPR, а также обязанности разработчиков и некоторые практические примеры по исполнению этих обязанностей
- Для Android-разработчиков: [обзор изменений в Android 10](#), касающиеся конфиденциальности пользователей и предоставления пользователям контроля над своей приватностью
- Для Apple-разработчиков: [документация по защите конфиденциальности пользователей](#), содержащая все - от концептуальных основ до отраслевых и государственных руководящих принципов, а также спецификации комплектов для разработки программного обеспечения
- Для разработчиков, использующих API-интерфейс Google (включая Google Sign-In): [условия предоставления услуг Google API](#), а также [политика в отношении пользовательских данных Google API Services](#)
- Для Facebook-разработчиков: [процедура реагирования на запрос](#) пользователя об удалении его персональных данных, [сервис ThreatExchange](#) и его настройки конфиденциальности, [публикация контактной информации о Data Protection Officer](#), [описание обновленных мер](#) по защите конфиденциальности пользователей при их аутентификации, [Общая политика платформы Facebook](#)
- Для разработчиков, использующих API-интерфейс Twitter: [руководство по конфиденциальности пользователей](#), которые охватывают варианты использования и настройки разрабатываемого ПО
- Для разработчиков, использующих Google Firebase: [документация Google Firebase по конфиденциальности и безопасности](#), которая включает описание примеров обработки персональных данных пользователей
- Для разработчиков, использующих GitHub: [Руководство разработчика](#), в котором рассказывается, как использовать REST API v3 в функциях защищенных веток, доступных в публичных репозиториях с GitHub Free, а также в публичных и частных репозиториях с GitHub Pro, GitHub Team и GitHub Enterprise Cloud

# Модернизация Конвенции 108 и влияние GDPR на РФ



## 1203 Внесение изменений в Конвенцию 108



На 128-ой сессии Комитета министров Совета Европы, состоявшейся 18.05.2018, был принят Протокол СДСЕ № 223, вносящий существенные изменения в Конвенцию и превращающие ее в «**Конвенцию 108+**», в том числе, и в сфере гармонизации многих положений Конвенции с нормами GDPR.

Для вступления Конвенции 108+ в силу необходимо, чтобы все участники действующей Конвенции (53 государства на 01.10.2018) подписали Протокол 223. Протокол был открыт для подписания в Страсбурге 10.10.2018 в ходе четвертой части сессии Парламентской ассамблеи Совета Европы и подписан рядом государств, включая Великобританию, Германию, Ирландию, Испанию, Нидерланды, Норвегию, Португалию, Францию, Швецию, **Россию**.

Если в течение пяти лет с даты открытия Протокола к подписанию 53 государство его не ратифицирует, то количество государств, требуемое для вступления Протокола в силу, будет уменьшено до 38 государств. Кроме того, согласно ст.37(3) Протокола сторона Конвенции может в момент подписания Протокола или в любой другой момент заявить, что она добровольно будет применять положения Протокола на временной основе.

### Полезные ссылки:

- [Текст Протокола](#)
- [Текст Конвенции с учетом Протокола](#)
- [Пояснительная записка к Протоколу](#)
- [Высокоуровневое описание изменений, вносимых Протоколом](#)
- [Таблица сопоставления старой и новой редакции Конвенции](#)

## 1204 Последствия принятия Конвенции 108+ для России



Согласно поручению Президента РФ, постоянный представитель России при Совете Европы Иван Солтановский от имени России в Страсбурге 10.10.2018 подписал Протокол СДСЕ № 223 об изменениях в европейскую Конвенцию о защите физических лиц при автоматизированной обработке персональных данных № 108.

Каждое государство-участник Конвенции 108+ будет обязано внести в свое национальное законодательство необходимые изменения для осуществления и эффективного применения положений Конвенции, определяющие следующие изменения в регулировании обработки и защиты персональных данных:

- вводятся понятия «контролер», «получатель» и «лицо, осуществляющее обработку данных»;
- закрепляется обязанность контролера своевременно уведомлять компетентный надзорный орган и субъектов об утечках персональных данных;
- фиксируется требование о внедрении механизмов защиты персональных данных при разработке процессов обработки данных (privacy by default) и при проектировании систем (privacy by design);
- национальные органы надзора должны быть независимыми от государственной воли и действовать самостоятельно;
- расширяется статус и полномочия Комитета Конвенции с консультативных до исполнительных и надзорных;
- и многое другое...

### ЧТО ИЗМЕНИТСЯ ДЛЯ РОССИИ ПОСЛЕ ПРИСОЕДИНЕНИЯ К МОДЕРНИЗИРОВАННОЙ КОНВЕНЦИИ СОВЕТА ЕВРОПЫ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

#### ОБЯЗАТЕЛЬСТВА РФ

- ✓ ГАРМОНИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА
- ✓ РАТИФИКАЦИЯ ПРОТОКОЛА И ПЕРЕДАЧА РАТИФИКАЦИОННОЙ ГРАМОТЫ В СОВЕТ ЕВРОПЫ

- 1** ТРЕБОВАНИЯ К ПРИНЦИПАМ ПРОПОРЦИОНАЛЬНОСТИ, МИНИМИЗАЦИИ И ЗАКОННОСТИ СБОРА, ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ (ПД) (УЖЕ СОДЕРЖАТСЯ В СТ. 5 ФЕДЕРАЛЬНОГО ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»)
- 2** ВВЕДЕНИЕ КАТЕГОРИИ «ГЕНЕТИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ» (ЗАКОНПРОЕКТ РАЗРАБАТЫВАЕТ РОСПОТРЕБНАДЗОР)
- 3** ОПРЕДЕЛЕНИЕ НОВЫХ ПРАВ, ПРЕДОСТАВЛЯЕМЫХ ГРАЖДАНАМ, ДЛЯ УПРАВЛЕНИЯ СВОИМИ ПД ПРИ ИХ ОБРАБОТКЕ НА ОСНОВЕ МАТЕМАТИЧЕСКИХ АЛГОРИТМОВ, ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И Т.Д.  
ОБЯЗАННОСТЬ ОПЕРАТОРОВ ПД УВЕДОМЛЯТЬ УПОЛНОМОЧЕННЫЙ НАДЗОРНЫЙ ОРГАН ОБ УТЕЧКАХ, УСТАНОВЛИВАЕТСЯ ЧЕТКИЙ РЕЖИМ ТРАНСГРАНИЧНЫХ ПОТОКОВ ДАННЫХ

#### ПОСЛЕДСТВИЯ

ДЛЯ ГРАЖДАН	ДЛЯ КОМПАНИЙ
<p>РАСШИРЕНИЕ ПРАВ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ О НЕЗАКОННОМ ДОСТУПЕ ТРЕТЬИХ ЛИЦ К ИХ ПЕРСОНАЛЬНЫМ ДАННЫМ</p> <p>люди имеют право не просто заявить о своем несогласии, но и независимо от гражданства и места жительства получать квалифицированную защиту от надзорного органа</p>	<p>С ПОДПИСАНИЕМ ПРОТОКОЛА РОССИЯ ПРИЗНАЕТСЯ ЕС СТРАНОЙ С АДЕКВАТНЫМ РЕЖИМОМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ. ЕВРОПЕЙСКИЕ РЕГУЛЯТОРЫ В РАМКАХ СОГРЕ НЕ БУДУТ ПРИМЕНЯТЬ К РОССИЙСКИМ КОМПАНИЯМ, РАБОТАЮЩИМ НА РЫНКАХ ЕС, ДОПОЛНИТЕЛЬНЫЕ МЕРЫ ЗАЩИТЫ ПД</p>

Какие главные изменения могут быть внесены в российскую нормативно-правовую базу?

1. Требования к принципам пропорциональности, минимизации и законности сбора, обработки и хранения персональных данных. Эти принципы уже содержатся в ст. 5 Федерального закона «О персональных данных».
2. Введение новой категории чувствительных данных – генетических данных. Роспотребнадзором разработан законопроект по включению генетических данных в понятие «Специальные категории персональных данных».
3. Определение новых прав, предоставляемых гражданам, для управления своими персональными данными при их обработке на основе математических алгоритмов, искусственного интеллекта и т.д. Также вводится обязанность операторов персональных данных уведомлять уполномоченный надзорный орган об утечках, устанавливается четкий режим трансграничных потоков данных.

# Законопроект о ратификации РФ протокола СДСЕ № 223 к Конвенции 108

проект

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

## О ратификации Протокола о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных

Ратифицировать Протокол о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (далее – Протокол), подписанный от имени Российской Федерации в г. Страсбурге 10 октября 2018 года, со следующими заявлениями:

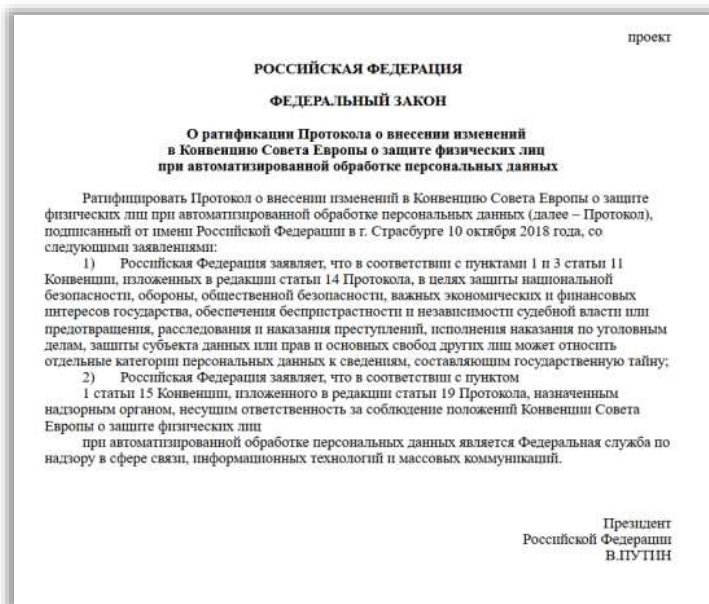
1) Российская Федерация заявляет, что в соответствии с пунктами 1 и 3 статьи 11 Конвенции, изложенных в редакции статьи 14 Протокола, в целях защиты национальной безопасности, обороны, общественной безопасности, важных экономических и финансовых интересов государства, обеспечения беспристрастности и независимости судебной власти или предотвращения, расследования и наказания преступлений, исполнения наказания по уголовным делам, защиты субъекта данных или прав и основных свобод других лиц может относиться отдельные категории персональных данных к сведениям, составляющим государственную тайну;

2) Российская Федерация заявляет, что в соответствии с пунктом 1 статьи 15 Конвенции, изложенного в редакции статьи 19 Протокола, назначенным надзорным органом, несущим ответственность за соблюдение положений Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Президент  
Российской Федерации  
В.ПУТИН

17.09.2019 был опубликован проект федерального закона «О ратификации Протокола о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

## Законопроект о внесении изменений в Федеральный закон «О персональных данных»



19.05.2020 был опубликован проект федерального закона о внесении изменений в Федеральный закон «О персональных данных», подготовленный в целях приведения положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в соответствии с положениями Протокола о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных подписанного от имени Российской Федерации в г. Страсбурге 10 октября 2018 г.

Необходимость оптимизации подходов к деятельности по обработке персональных данных, недостаточная проработанность действующих правовых условий, обеспечивающих сохранение юридических гарантий прав и законных интересов государства, общества и граждан.

Планируемый срок вступления проекта нормативного правового акта в силу: **январь 2021 г.**

## Конвенция об иностранных судебных решениях по гражданским или торговым делам

Главная > Новости > Принята Конвенция о признании и приведении в исполнение иностранных судебных решений по гражданским или торговым делам

**ПРИНЯТА КОНВЕНЦИЯ О ПРИЗНАНИИ И ПРИВЕДЕНИИ В ИСПОЛНЕНИЕ ИНОСТРАННЫХ СУДЕБНЫХ РЕШЕНИЙ ПО ГРАЖДАНСКИМ ИЛИ ТОРГОВЫМ ДЕЛАМ**



2 июля 2019 г. завершилась 22-я Дипломатическая сессия Гаагской конференции по международному частному праву.

Руководителем российской правительственной делегации, Уполномоченным Российской Федерации при Европейском Суде по правам человека – заместителем Министра юстиции Российской Федерации М.Л. Гальпериным подписан заключительный акт Сессии, итогом которой стало принятие Конвенции о признании и приведении в исполнение иностранных судебных решений по гражданским или торговым делам (Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters).

Главной целью Конвенции является создание предсказуемого и эффективного режима трансграничного исполнения вынесенных судебных решений по гражданским и торговым делам. Отсутствие до настоящего времени универсального международного договора, который позволял бы приводить в исполнение решения национальных судов на территории иностранных государств, негативно сказывалось на привлекательности государственного правосудия как механизма разрешения споров с иностранным элементом. Принятая Конвенция призвана восполнить этот пробел.

Несмотря на то что ряд категорий дел исключен из сферы действия Конвенции (семейные споры, споры по делам о несостоятельности (банкротстве), споры в области интеллектуальной собственности), сам инструмент Конвенции носит универсальный характер и полностью регулирует процедуру трансграничного исполнения вынесенных судебных решений. В частности, в ней прописаны основания как для признания и приведения в исполнение решений, так и для отказа в выдаче экзекютуры, а также определяется исключительная юрисдикция судов.

Более подробно с текстом Конвенции можно ознакомиться на [сайте Гаагской конференции по международному частному праву](http://www.hcch.net).

02 июля 2019 года

02.07.2019 завершилась 22-я Дипломатическая сессия Гаагской конференции по международному частному праву.

Руководителем российской правительственной делегации, Уполномоченным Российской Федерации при Европейском Суде по правам человека – заместителем Министра юстиции Российской Федерации М.Л. Гальпериным подписан заключительный акт Сессии, итогом которой стало принятие **Конвенции о признании и приведении в исполнение иностранных судебных решений по гражданским или торговым делам** (Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters).

Главной целью Конвенции является создание предсказуемого и эффективного режима трансграничного исполнения вынесенных судебных решений по гражданским и торговым делам. Несмотря на то что ряд категорий дел исключен из сферы действия Конвенции (семейные споры, споры по делам о несостоятельности (банкротстве), споры в области интеллектуальной собственности), сам инструмент Конвенции носит универсальный характер и полностью регулирует процедуру трансграничного исполнения вынесенных судебных решений.



## Заявление датского DBA о трансграничной передаче данных пользователей веб-сайтов в РФ



Датское управление по делам бизнеса ("DBA") 13.06.2022 опубликовало заявление об обмене данными пользователей веб-сайтов с российскими компаниями посредством использования файлов cookie, шрифтов, изображений и других плагинов, в частности, после освещения этого вопроса в СМИ.

DBA провел анализ, чтобы получить представление о масштабах проблемы, проанализировав 10,000 веб-сайтов с наибольшим количеством посещений в Дании и изучив, сколько из них автоматически делились данными о пользователях своих сайтов с российскими компаниями в первом квартале 2022 года. Анализ показал, что около 3% посещаемых датчанами веб-сайтов делились данными с третьими лицами из РФ. В среднем данные о примерно 3,7 млн. посещений датских веб-сайтов ежемесячно передаются российским сторонним службам.

DBA подчеркнул, что зачастую граждане не знают о такой практике обмена данными, поскольку их данные собираются без предварительного согласия. В связи с этим DBA описал шаги, которые пользователи веб-сайтов могут предпринять для своей защиты, включая:

- ◇ удаление файлов cookie на веб-сайтах;
- ◇ использование VPN для маскировки и постоянного изменения IP-адресов пользователей веб-сайтов;
- ◇ использование интернет-браузеров со встроенными функциями конфиденциальности и безопасности.

## Финляндия и Норвегия временно запретили «Яндексу» передавать данные клиентов такси Yango в Россию

◇ Уполномоченный по защите персональных данных Финляндии Ану Талус [запретила](#) передавать данные пользователей службы такси Yango, которая является дочерним брендом ООО "Яндекс", в Россию на фоне законодательной реформы в РФ. Уполномоченный считает, что Yango не может обеспечить защиту персональных данных в соответствии с законодательством ЕС, особенно после законодательной реформы в России. В связи с этим необходимо принятие решения о приостановке передачи и запрете обработки персональных данных", - указано в документе. Уточняется, что запрет вступит в силу с 27.09.2023 и будет действовать до 30.11.2023. Сбором и обработкой персональных данных для Yango занимается компания Ridetech International B.V., базирующаяся в Нидерландах. К персональным данным относятся, в частности, геопозиция клиента и адрес поездки.

◇ Правительство Финляндии [не будет ограничивать](#) работу принадлежащего "Яндекс такси" сервиса Yango на территории страны. По оценке финского агентства транспорта и связи Traficom, передача пользовательских данных сервису Yango "не представляет реальной угрозы безопасности". Финский уполномоченный по защите персональных данных [отменил запрет](#) Yango на передачу персональных данных в Россию. Российский закон, обязывающий агрегаторы такси предоставлять ФСБ доступ к данным пассажиров, не распространяется на деятельность Yango в Финляндии. Отслеживание передачи данных Yango, однако, продолжится, несмотря на это решение.

◇ Норвегия вслед за Финляндией [запретила](#) «Яндексу» передачу и обработку данных пользователей в Россию, которые собираются в службе такси Yango. По мнению Управления по защите данных Норвегии, «это создает серьезный риск для конфиденциальности, поскольку российские власти потенциально могут отслеживать передвижения жителей Норвегии через Yango». Управление сотрудничает с органами по надзору за данными в Финляндии и Нидерландах по этому вопросу. Кроме того, ведомство выделило для Yango время до 14.08.2023 для разъяснений.

◇ Нидерланды начали [расследование](#) в отношении сервиса такси Yango, принадлежащего Yandex NV. Расследование связано с российским законом, который вступил в силу с 1 сентября и обязал отечественные сервисы такси передавать ФСБ данные о поездках клиентов. Голландские власти опасаются, что из-за него в руки российских спецслужб попадут данные нидерландцев, которые пользуются Yango.

◇ В пресс-службе «Яндекса» [заявили](#), что российские правоохранители не могут получать доступ к данным о поездках пользователей вне России. «Данные о поездках могут получить исключительно правоохранительные органы той страны, где поездка была совершена, по процедурам, прописанным в локальных законах», – уточнили в представительстве.



Этот смелый эскиз называется «Заяц, начитавшийся Байрона GDPR, в бурную ночь на утёсе вглядывается в бушующую бездну».

*Мел, стенка, 1X1.*



**Алексей Мунтян, 16 лет в Data Privacy**

Основатель и CEO в компании Privacy Advocates

Соучредитель в Russian Privacy Professionals  
Association - RPPA.ru

Внешний Data Protection Officer в нескольких  
транснациональных холдингах

**+7 (903) 762-64-15**

**[alexey.muntyan@privacy-advocates.ru](mailto:alexey.muntyan@privacy-advocates.ru)**



Telegram-канал