



Written by Daniel J. Solove

www.teachprivacy.com

Illustrated by Ryan Beckwith

Рассмотрение механизмов и специфики применения | Алексей Мунтян
Генерального регламента ЕС о защите данных (GDPR) | Редакция от 28.12.2020



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

2 Присоединяйтесь к Russian Privacy Professional Association!



Регистрация в RPPA
<https://rppa.ru/rppa/reg>



rppa.ru



[Facebook](#)



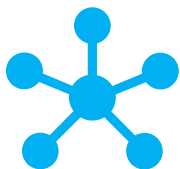
[LinkedIn](#)



[Instagram](#)



[Telegram](#)



1

Комьюнити

Объединение специалистов по приватности из России, Восточной Европы и Азии:

- создание единой стратегии
- определение подходов по выполнению требований применимого законодательства в области обработки и защиты ПДн



2

Регуляторы

Взаимодействие с локальными регуляторами по вопросам обработки и защиты ПДн:

- ответы на вопросы,
- комментарии по тем или иным законодательным нормам,
- уточнение и определение единой стратегии и подходов.



3

Обмен опытом

Взаимодействие с другими ассоциациями и объединениями в области приватности.



4

Мероприятия

Организация мероприятий:

- объединение специалистов по приватности,
- обмен опытом,
- обсуждение вопросов в области приватности.



5

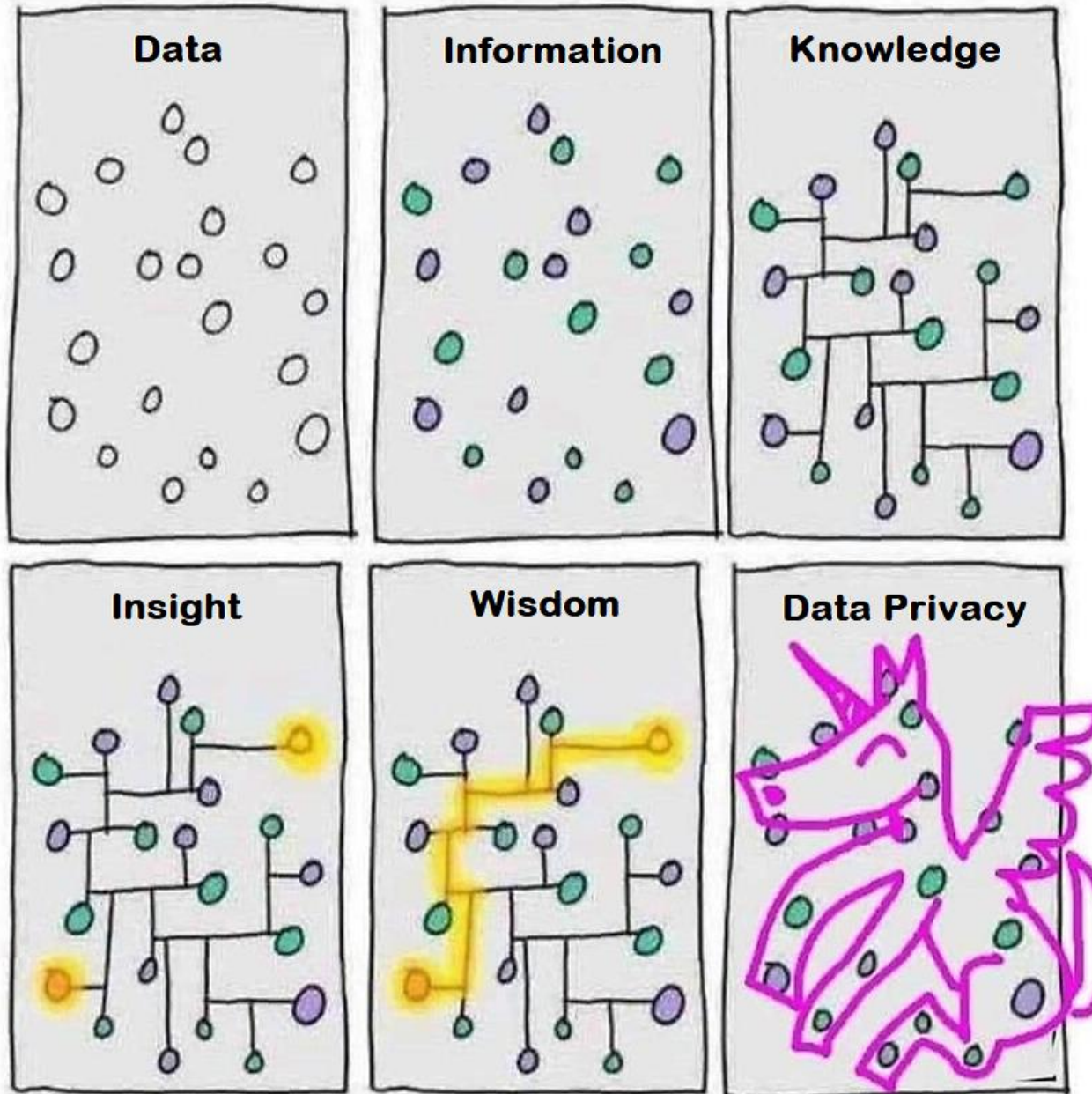
Материалы

Разработка, обновление и адаптация руководств и разъяснений по вопросам применения законодательных требований в области обработки и защиты ПДн с привлечением участников Ассоциации.

3 Содержание



1. [Обзор контекста принятия и механизмов GDPR](#)
2. [Территориальная сфера действия GDPR и трансграничная передача данных](#)
3. [Рекомендации, руководства и практические пособия](#)
4. [Вспомогательная информация от коммерческих и некоммерческих организаций](#)
5. [Data Protection \(Privacy\) by Design and by Default](#)
6. [Data Protection Impact Assessment](#)
7. [Records of Processing Activities](#)
8. [Legitimate Interests](#)
9. [Data Breach](#)
10. [Data Protection Officer](#)
11. [Соглашения об обработке и защите данных](#)
12. [Взаимодействие с пользователями сайтов и приложений](#)
13. [Большие данные, искусственный интеллект и машинное обучение](#)
14. [Автоматизация Privacy и Data Protection](#)
15. [Защита персональных данных](#)
16. [Псевдонимизация и анонимизация](#)
17. [Международные стандарты](#)
18. [Правоприменительная практика](#)
19. [Штрафы - базы дел и аналитика](#)
20. [Штрафы - интересные кейсы](#)
21. [Иные санкции и меры принуждения](#)
22. [Судебная практика – базы решений и интересные ситуации](#)
23. [Влияние GDPR на бизнес](#)
24. [Итоги применения GDPR в 2018-2020 и дальнейшие перспективы](#)
25. [Законодательные инициативы о персональных данных в ЕС и США](#)
26. [Модернизация Конвенции 108 и ее влияние на регулирование в РФ](#)



Обзор контекста принятия и механизмов GDPR



6 Эволюция европейского законодательства о защите данных

2016 (EU)
EU-US PrivacyShield approved

2013 (OECD)
OECD Guidelines updated

2018 (CoE)
Convention 108 updated

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

1948 (UN)
The Universal Declaration of Human Rights



UN founded

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

1981 (CoE)
Convention 108

1973
First national privacy law: Data Act, Sweden

1980 (OECD)
OECD Guidelines

2000 (EU)
Safe Harbour decision (later overturned)

2001 (CoE)
Convention 108 amended

2002 (EU)
ePrivacy Directive

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

2009 (EU)
ePrivacy Directive amended

2016 (EU)
NIS Directive

2016 (EU)
Law Enforcement Directive

2016 (EU)
PNR Directive

20?? (EU)
ePrivacy Regulation

1970
First modern privacy law. Hesse, Germany

1979
Data protection laws enacted in 7 member states

1995 (EU)
Data Protection Directive

2000 (EU)
E-Commerce Directive

2006 (EU)
Data Retention Directive (later repealed)

2016 (EU)
GDPR

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

2004 Madrid bombings

2005 London bombings

Edward Snowden disclosures about global surveillance

Max Schrems

#me too

Reflection in Germany of Gestapo's privacy abuses in WW2 and Stas's privacy abuses in East Germany

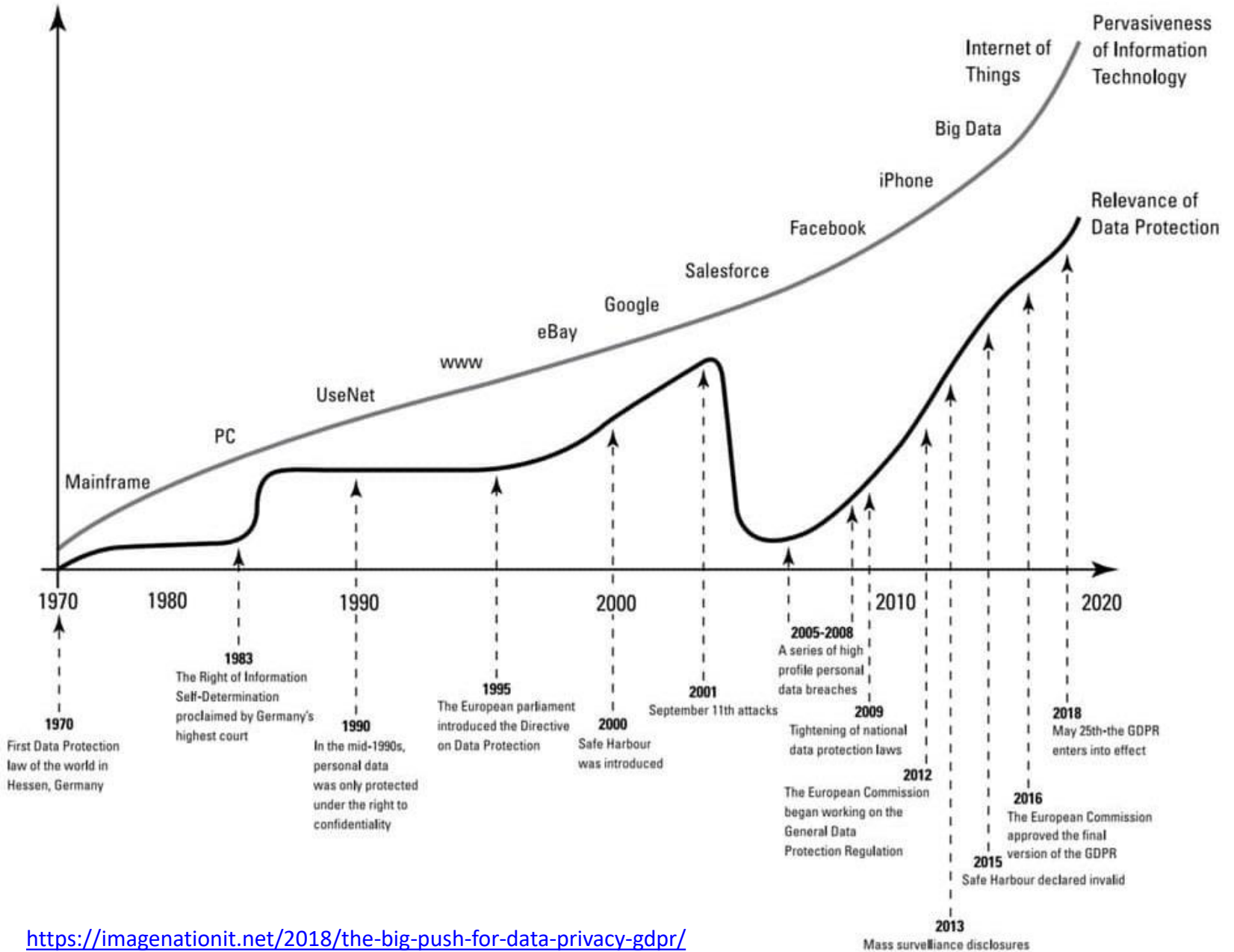
Revelations about global surveillance & existence of NSA and GCHQ

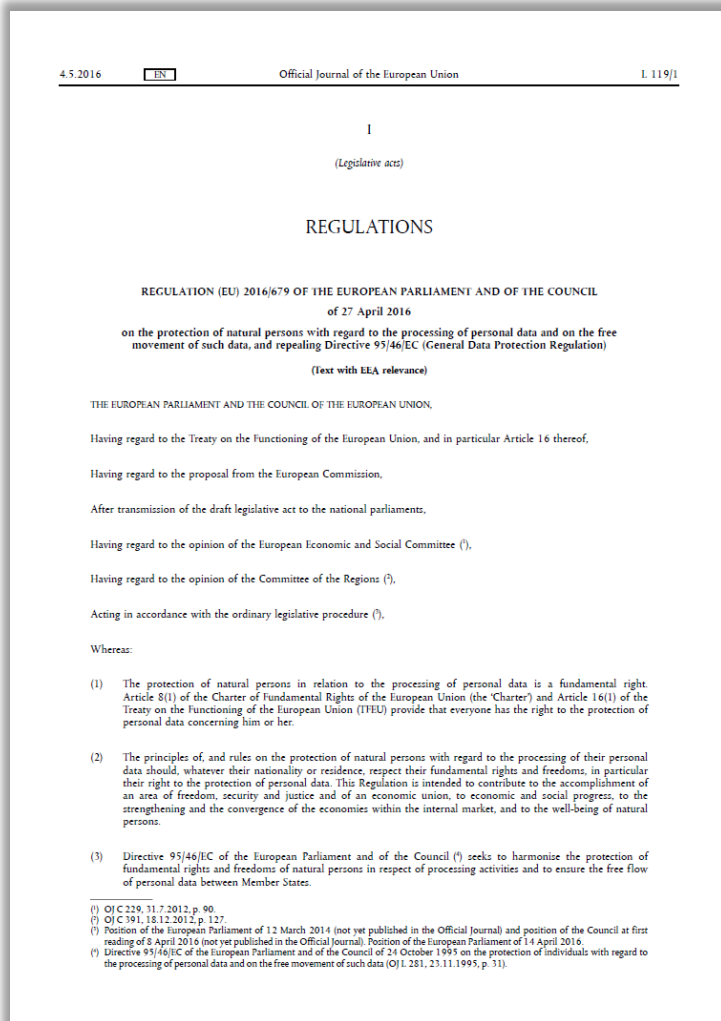
High profile data breaches and/or concerns

cardsystems, SONY, ebay, EQUIFAX, YAHOO!, T.J-maxx, EVERNOTE, HM Revenue & Customs, Adobe, UBER, AOL, Cambridge Analytica

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

Social Media Trends





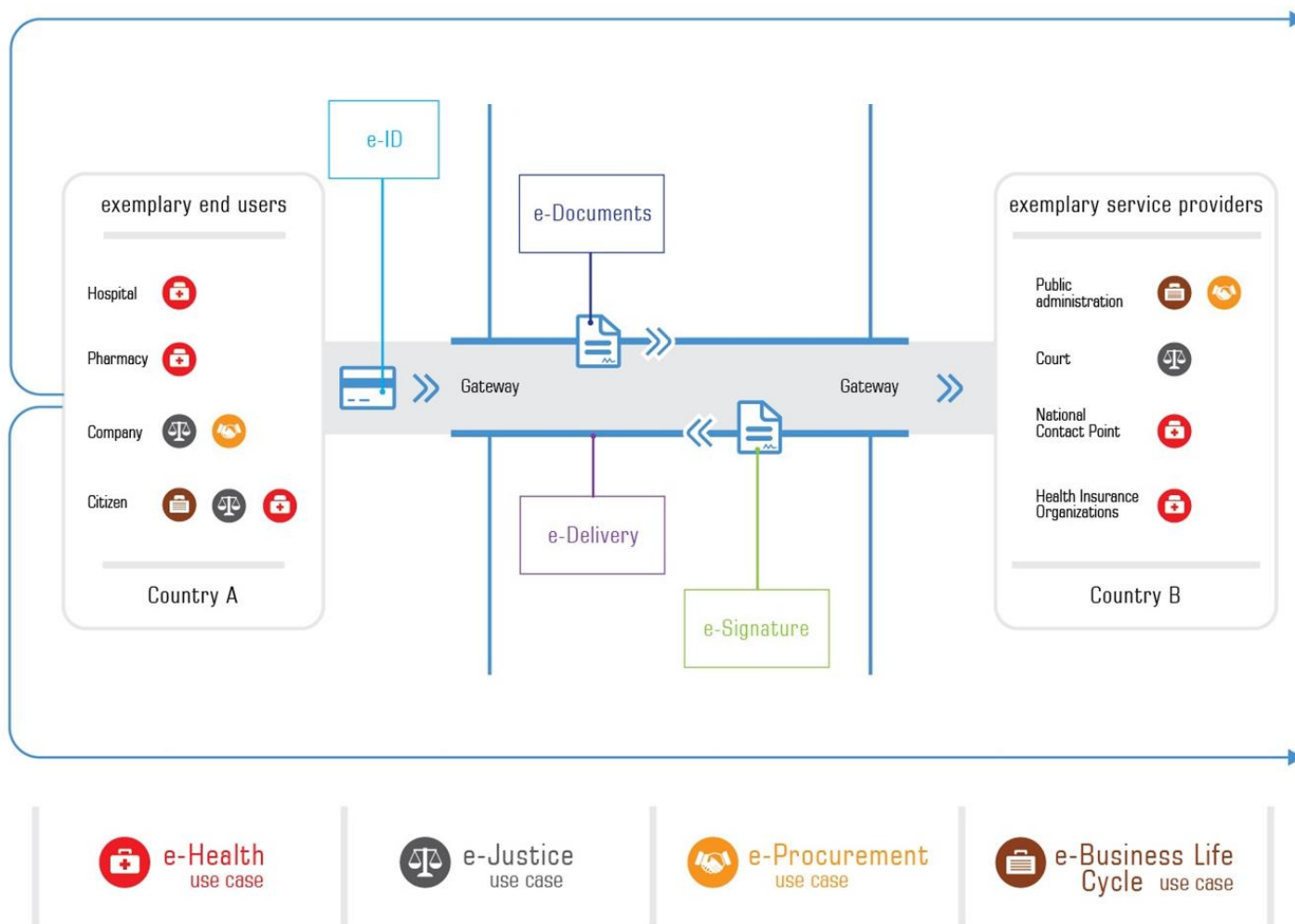
[Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**) – это новый 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
- 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)

9 GDPR как часть Digital Single Market Strategy

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 онлайнowych бизнес-проектов, доступность контента пользователям, защищенность интересов авторов.



10 GDPR как часть реформы европейского права



- [Regulation \(EU\) 910/2014](#) of 23 July 2014 (**electronic IDentification, Authentication and trust Services Directive – eIDAS**) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- [Directive \(EU\) 2016/680](#) of 27 April 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 8 June 2016 (**Trade Secrets Directive – TSD**) on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
- [Directive \(EU\) 2016/1148](#) of 6 July 2016 (**Networking and Information Security Directive – NISD**) concerning measures for a high common level of security of network and information systems across the Union
- [Regulation \(EU\) 2018/1725](#) of 23 October 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
- [Regulation \(EU\) 2018/1807](#) of 14 November 2018 (**Free Data Movement – FDM**) on a framework for the free flow of non-personal data in the European Union
- [Regulation \(EU\) 2019/881](#) of 17 April 2019 (**Cybersecurity Act**) on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
- [Regulation \(EU\) 2019/1150](#) of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services + [Guidelines on ranking transparency](#)

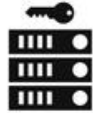
Полезные ссылки:

- [общее описание реформы правил по защите данных в ЕС;](#)
- [национальные органы стран-участниц ЕС по защите данных;](#)
- [иконографика по GDPR от Европейской Комиссии;](#)
- [подробное руководство по GDPR от Information Commissioner's Office \(UK\);](#)
- [удобный навигатор по тексту GDPR, показывающий связь между статьями и пунктами преамбулы;](#)
- [перечень стран, обеспечивающих адекватный уровень защиты данных](#) (Аргентина, Канада, Израиль, Новая Зеландия, Швейцария, Уругвай, США и [Япония](#) + продолжаются переговоры с Южной Кореей);
- [разъяснения шведского DPA](#) о трансграничной передаче персональных данных за пределы ЕС/EACT.

11 На что еще стоит обратить внимание в контексте GDPR



- С [20.07.2018](#) GDPR регулирует обработку и защиту персональных данных не только в ЕС, но и в иных странах, которые осуществили имплементацию норм GDPR – такие правовые акты приняты в [Норвегии](#), [Лихтенштейне](#), [Исландии](#) в рамках [Европейской ассоциации свободной торговли](#) (за исключением Швейцарии).
- 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).
- 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.
- [Материалы](#) Международной конференции уполномоченных по защите данных и конфиденциальности (International Conference of Data Protection and Privacy Commissioners), которая проводится на ежегодной основе с 1979 года под эгидой Европейского инспектора по защите данных ([European Data Protection Supervisor](#)).
- Термины и определения в области data protection: [словарь EDPB](#) и [словарь IAPP](#)
- [Standard contractual clauses](#) for data transfers between EU and non-EU countries
- [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)
- [The Data Protection Act 2018 \(United Kingdom\)](#)
- [The Federal Data Protection Act \(Germany\)](#)
- [The Data Protection Law n°2018-493 \(France\)](#)
- [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 \(Ireland\)](#)



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

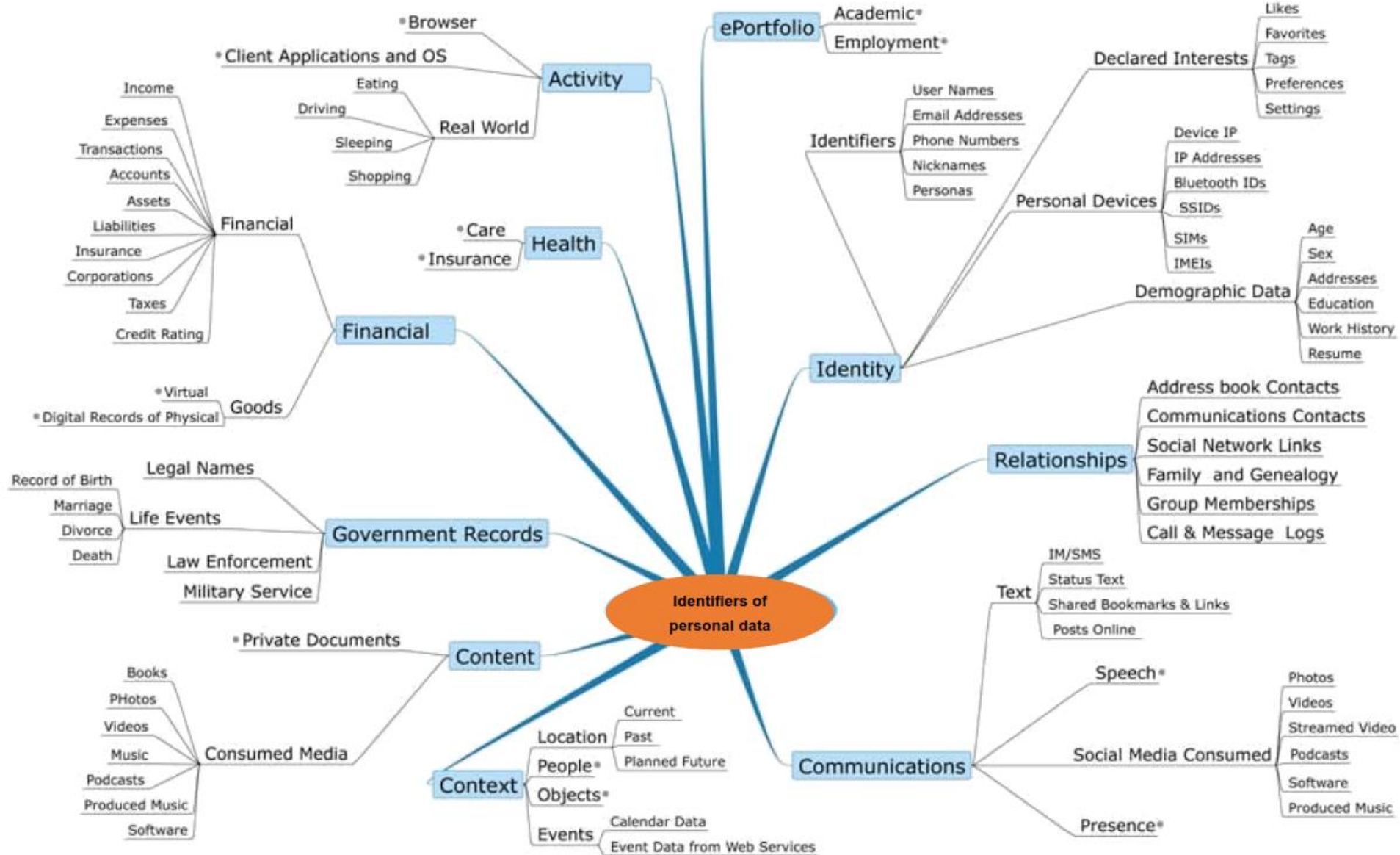
Include data provided by the electronic devices we use: mobiles, cookies identifiers, IP address, others.



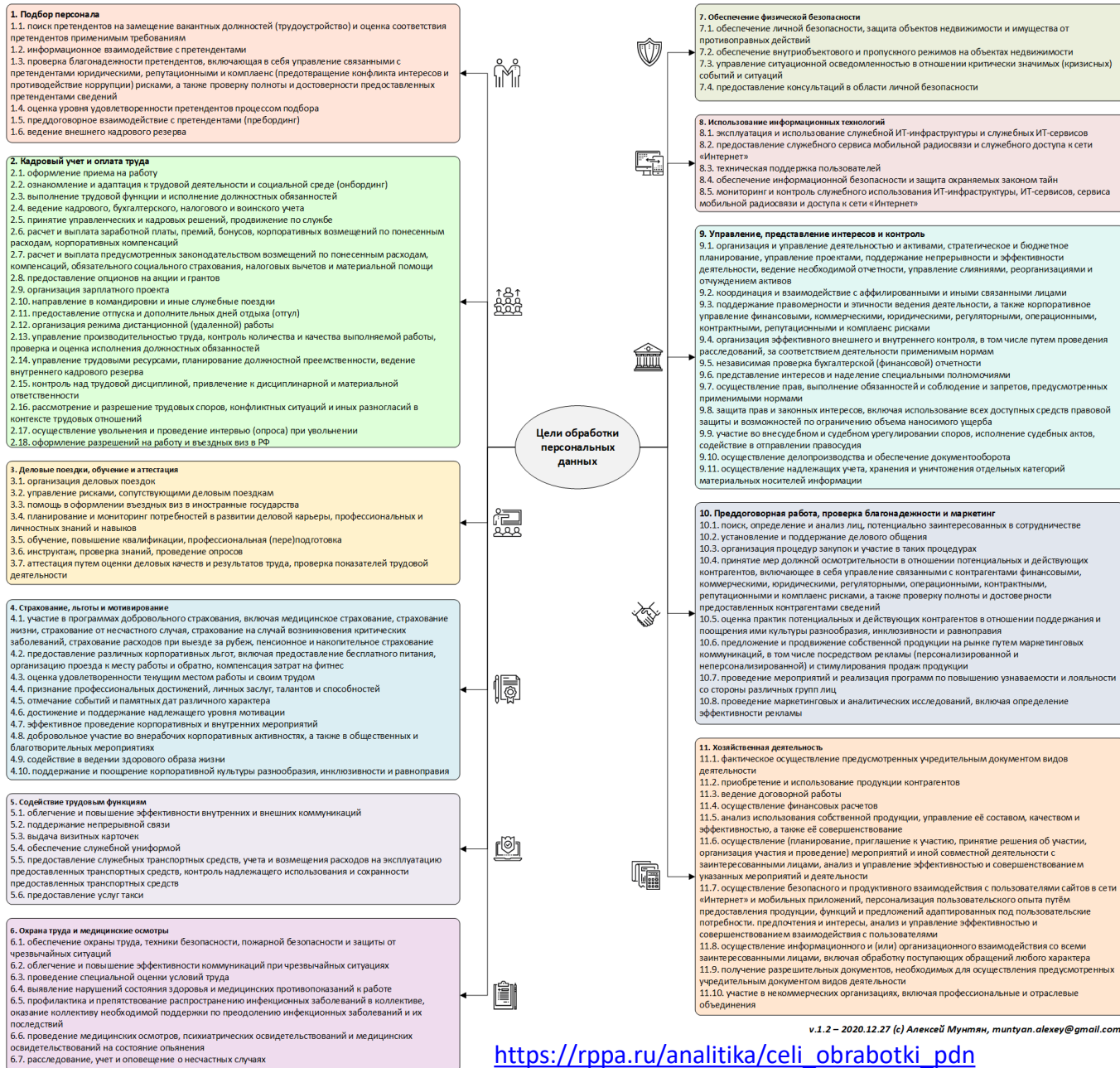
TO ONE OR MORE FACTORS

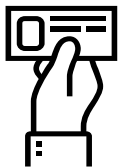
Include data that when combined with unique identifiers and other info create a profile and identify a person.

13 Пример категоризации персональных данных



Цели обработки персональных данных - 92 процессинговых активности, объединенные в 11 доменов





Предоставленные данные

получены от субъектов или их представителей, например, заполнение веб-форм на сайте, представление интересов в суде



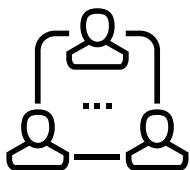
Распространенные данные

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



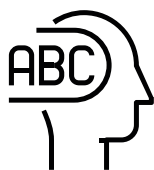
Наблюдаемые данные

зафиксированы путем отслеживания действий, например, онлайн-трекинг, геолокация, видеонаблюдение



Принятые данные

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



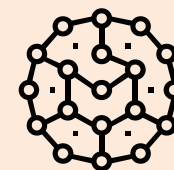
Назначенные данные

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



Производные данные


созданы путем простого анализа других данных, например, расчет прибыльности клиента по количеству посещений и купленных товаров



Предполагаемые данные


созданы путем продвинутого анализа наборов данных, например, расчет кредитного рейтинга или прогнозирование состояния здоровья

Профилирование




Have the guts to tell to your customers what the hell are you doing with their data and why ... Hopefully you have a legit purpose. If you don't... don't bother about the rest'

#transparency
#ACCOUNTABILITY




Speak them clearly, don't hide beyond legal bullshit, like "for example, but not limited to... blah, blah, blah";

#transparency




Be as specific as possible. Don't use as a reason for processing personal data on your site, "To improve use experience...". Nobody would believe this anyway:

#fairness
#lawfulness




If you just want to add a new processing to your business, let them decide if they're interested. They trusted you for one job, one purpose. You have to earn their trust and/or consent for other purposes.

#scopelimitation




Also, let them know when you share data with others and why. Sharing data could be also using online tools and services;

#transparency
#scopelimitation



Don't bite more than you can (you're allowed to) chew. If you're not really needing the data, don't ask. Some things are none of your business, if you don't need them to deliver your service.

#dataminimization




Take care of their data as of your own... or even better. But not all data are equal. Some are more sensitive than others. We all have "secrets". Keep their "secrets" even safer, if they shared them with you

#integrity
#confidentiality




Keep data clean, updated and available. Don't become a data hoarder. When this are of no specific use... drop them;

#accuracy
#storagelimitation



Tell them what personal data stored so far. They deserve to know. If they don't like you... or your services, let them go. Don't insist man! Let them go if they want... and never bother them again. Also, tell them if you share with others and why?

#fairness
#transparency



If something happened to their data, despite your best efforts and it could become ugly (you know shit happens) let them know before they could run into problems.

#integrity

TERRITORIAL SCOPE



EU Establishments

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

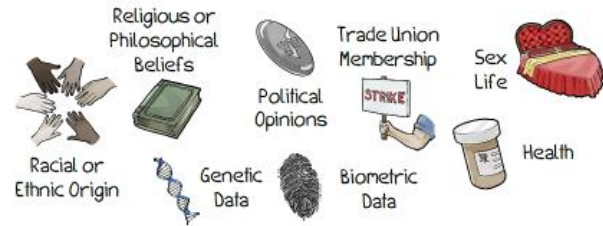
THE PLAYERS



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.

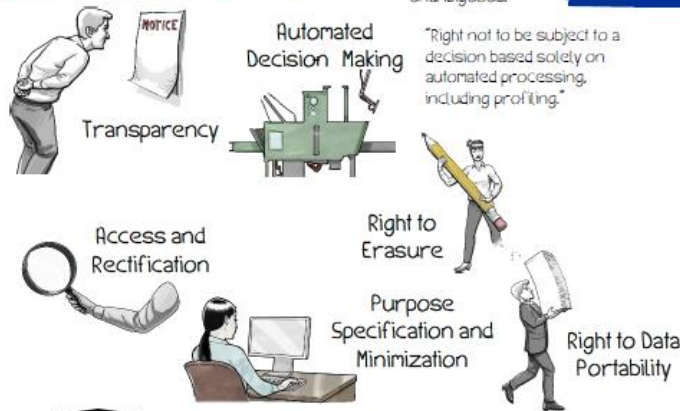


DATA BREACH NOTIFICATION

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

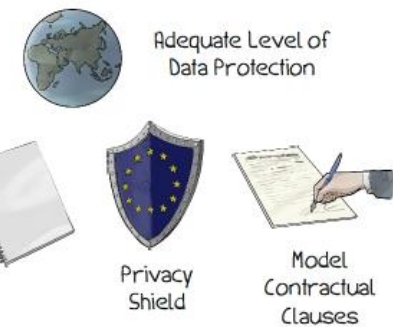


ENFORCEMENT

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



What organizations have to do



Keep records of all processing of personal information



Institute safeguards for cross-border data transfers



Maintain appropriate data security



Collect personal data lawfully and fairly, and where relevant, get appropriate consent and provide notification of personal data processing activities



Get a parent's consent to collect data for children under 16



Consult with regulators before certain processing activities



Provide appropriate data protection training to personnel having permanent or regular access to personal data



Conduct Data Protection Impact Assessments on new processing activities



Implement Data Protection-by-Design (Privacy "baked-in")



Take responsibility for the security and processing activities of third-party vendors



Appoint a Data Protection Officer (if you regularly process lots of data, or particularly sensitive data)



Be able to demonstrate compliance on demand



Notify data protection agencies and affected individuals of data breaches in certain circumstances

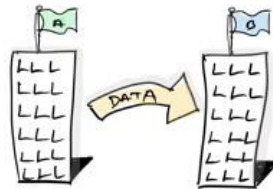
What individuals can do



Withdraw consent for processing



Request a copy of all of their data & request corrections if wrong



Request the ability to move their data to a different organization



Request that their information is deleted when there's no purpose to retain it



Object to automated decision-making processes, including profiling

What regulators can do



Ask for records of processing activities and proof of steps taken to comply with the GDPR



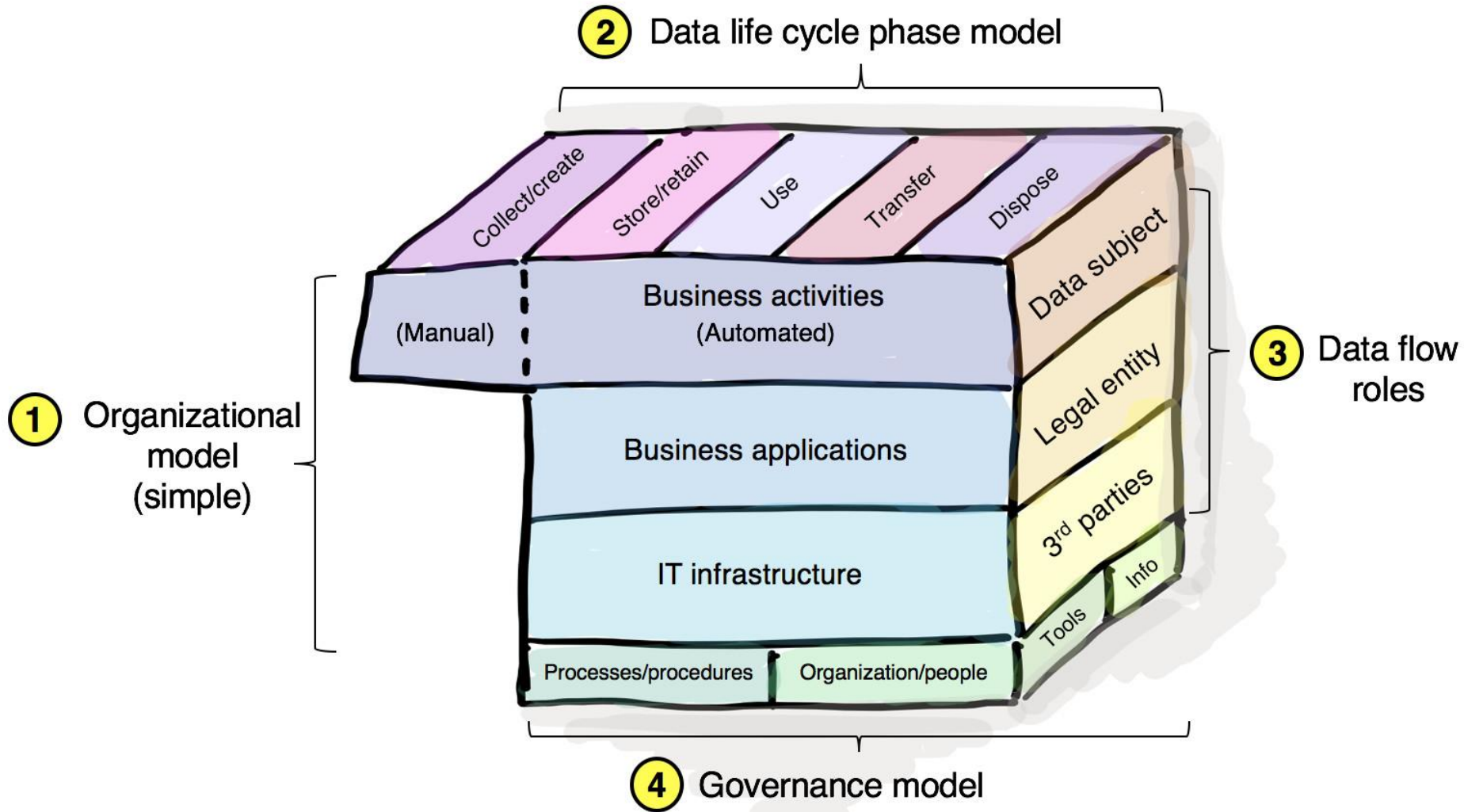
Suspend cross-border data flows



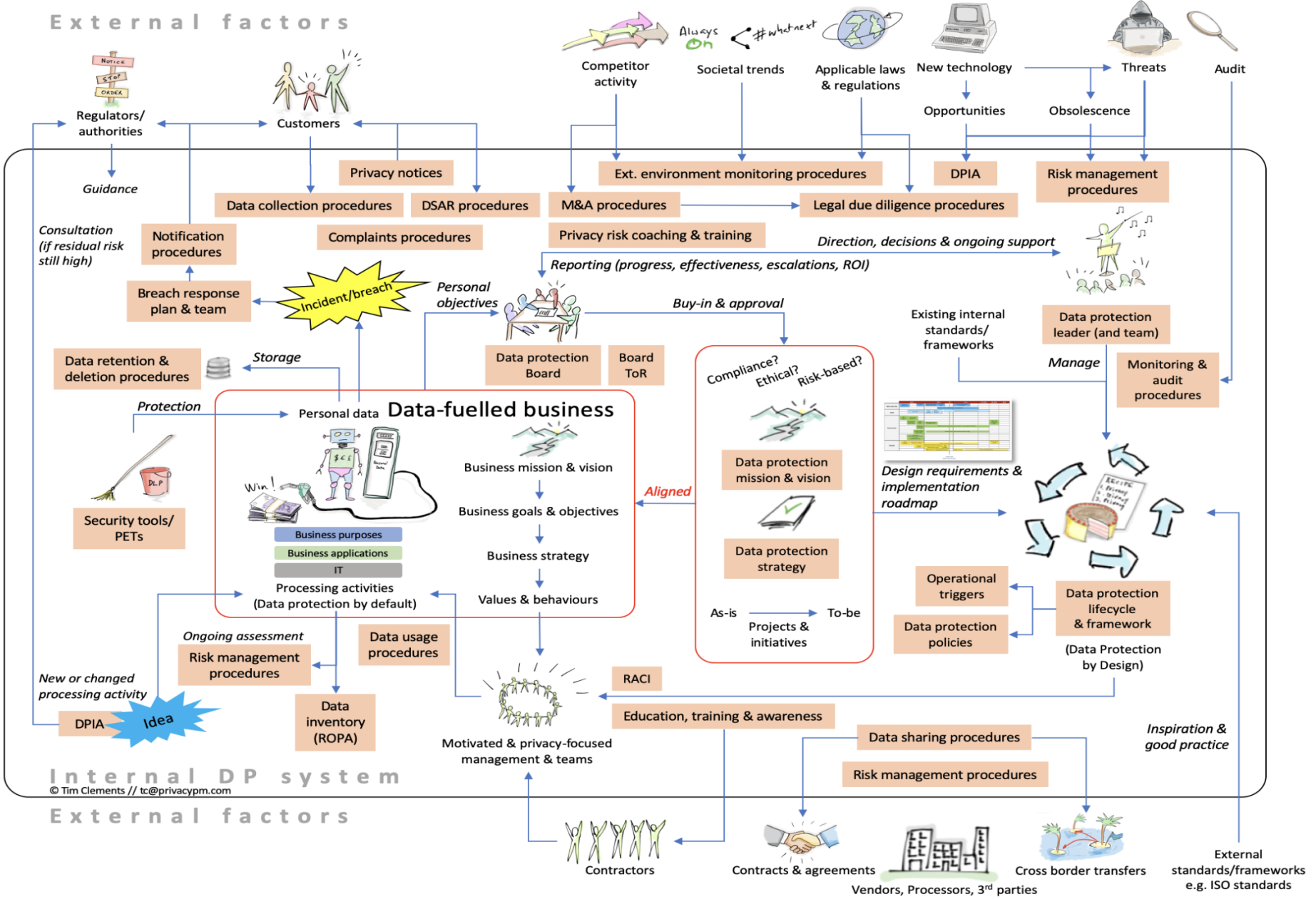
Impose temporary data processing bans, require data breach notification, or order erasure of personal data



Enforce penalties of up to €20 million or 4% of annual revenues for non-compliance



Представление системы управления обработкой и защитой персональных данных в организации



- 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 Assessment¹ (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»)

¹ См. заключение EDPB - https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

- 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 персональные данные (Art.16)
- Право на удаление персональных 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 обработчик (Art.79)
- Право на представительство (передачу полномочий) (Art.79)
- Право на компенсацию материального или нематериального ущерба (Art.82)

Территориальная сфера действия GDPR и трансграничная передача данных



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 Жаров на VIII Международной конференции по защите персональных данных».

По его словам, участницей меж...

устанавливающих порядок обработки персональных данных и «Регламент, по нашему мнению, должен учитываться только по отношению к европейским гражданам российскими операторами на территории России», отметив, что такая позиция соответствует общепринятым международным принципам обработки персональных данных. «Считаю, что к вопросу о применимости Регламента ЕС будет вернуться только после его вступления в законную силу, то есть после его правоприменения. И когда это будет зафиксировано в международном договоре, подчеркнул А. Жаров.

Конференция «Защита персональных данных» проводится по инициативе 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>




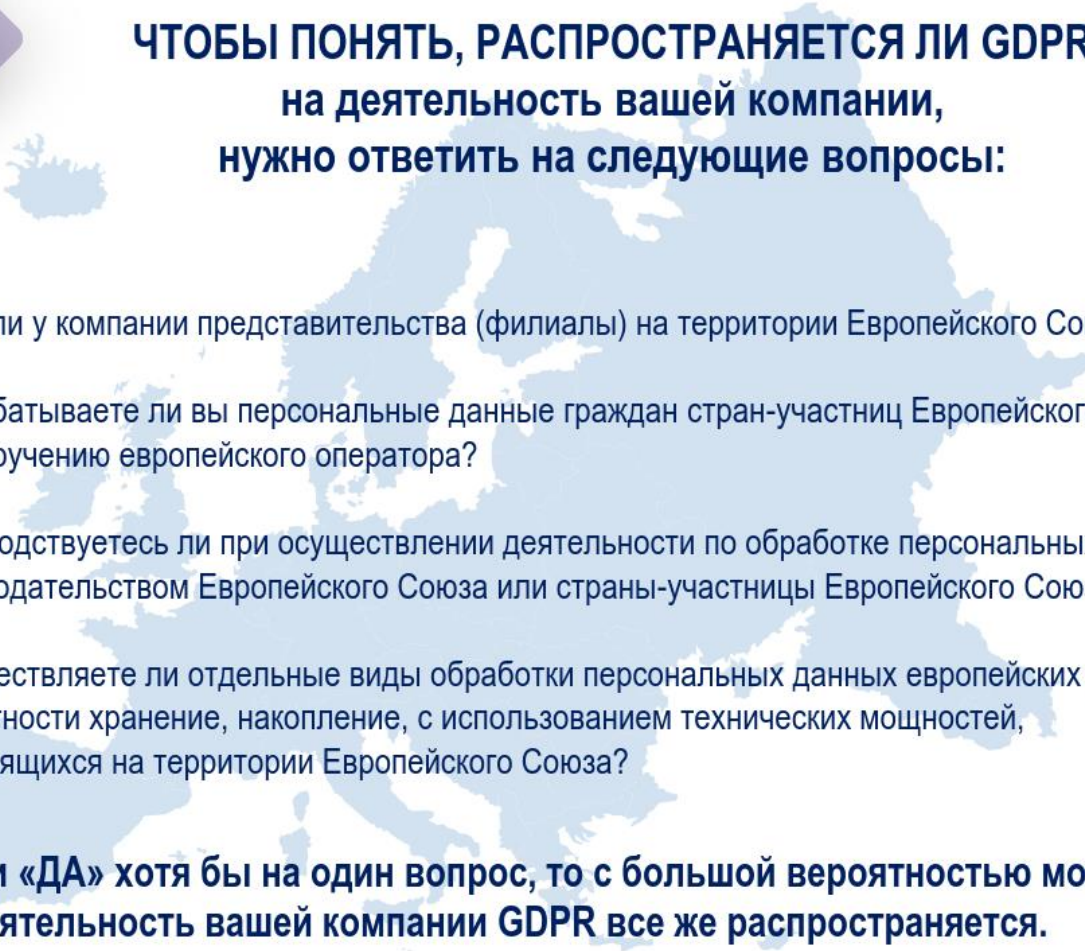

Консультативный совет при Уполномоченном органе по защите прав субъектов персональных данных в 2018 году планирует представить предложения по правовому статусу «обезличенных» данных, а также по возможной корректировке законодательства о персональных данных в контексте реализации программы «Цифровая экономика».

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 в Общем регламенте 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 деятельность 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.

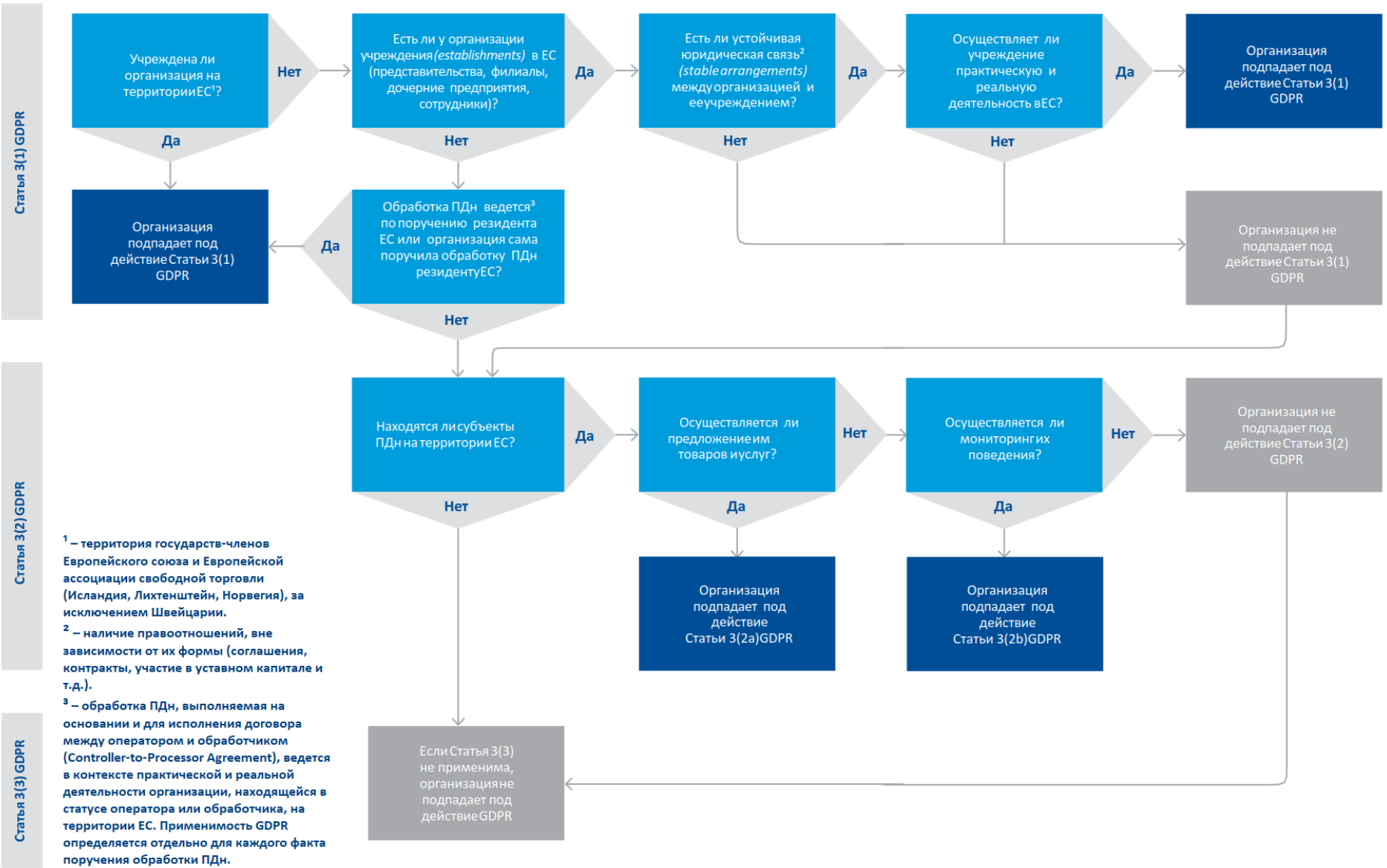


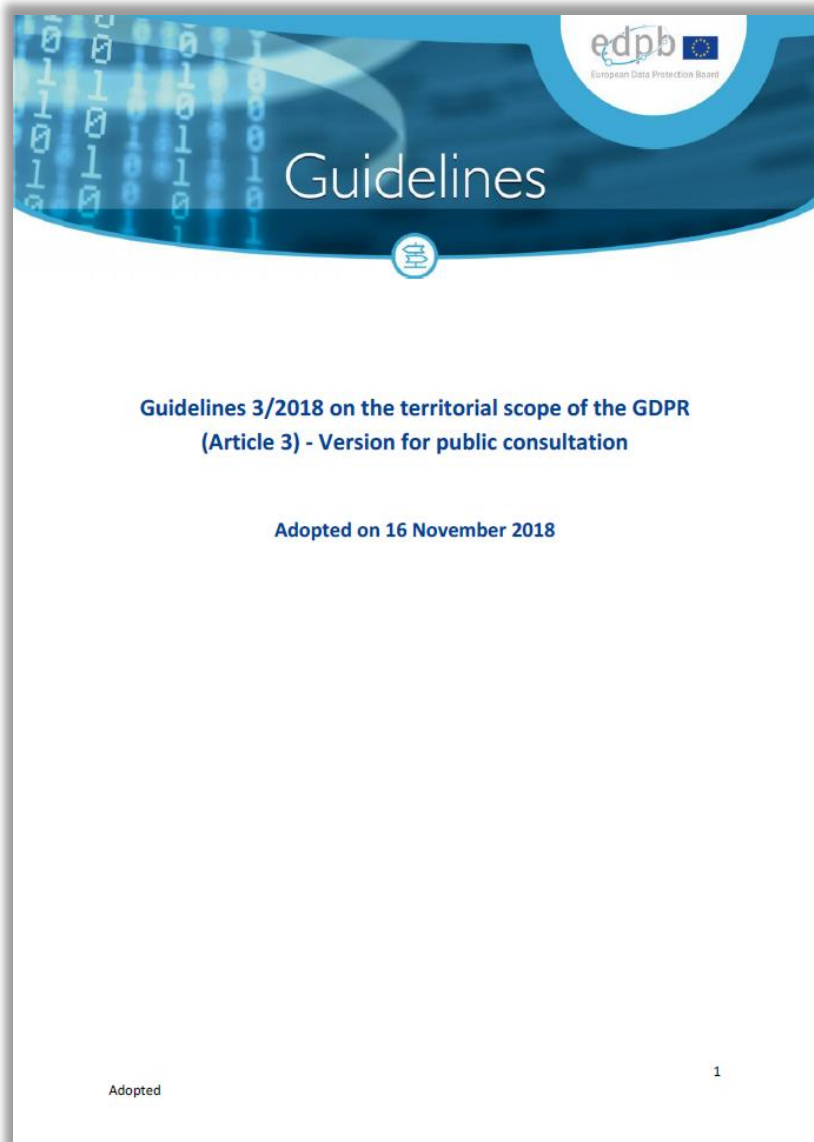
ЧТОБЫ ПОНЯТЬ, РАСПРОСТРАНЯЕТСЯ ЛИ GDPR на деятельность вашей компании, нужно ответить на следующие вопросы:

- ★ Есть ли у компании представительства (филиалы) на территории Европейского Союза?
- ★ Обрабатываете 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.

Принципиальная высокоуровневая схема оценки применимости положений GDPR к отдельным процессам обработки персональных данных, подготовленная коллегами из KPMG со скромным участием автора презентации.





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»](#).



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

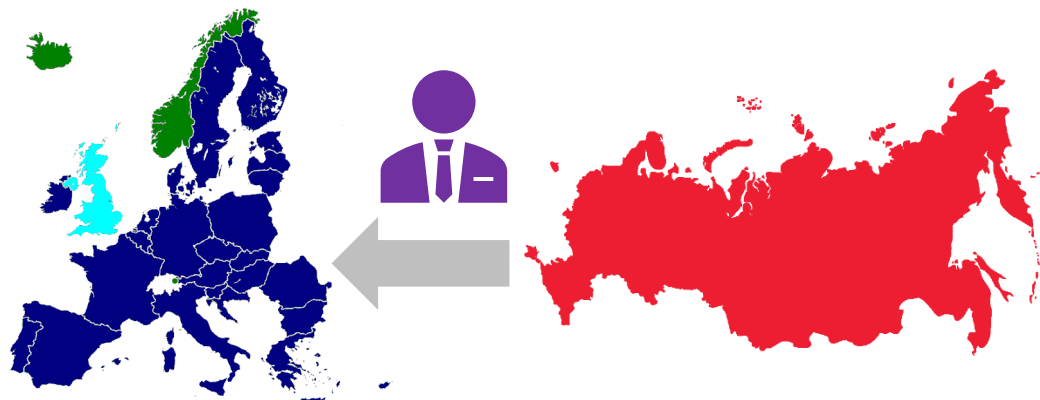


В случае отсутствия решения согласно Статье 45(3) контролер или обрабатывающее данные лицо могут передать персональные данные третьей стране или международной организации только, если контролер или обрабатывающее данные лицо предусмотрели соответствующие гарантии и если субъекты данных обладают юридически 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.

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

Inside Privacy

Updates on developments in data privacy and cybersecurity

FROM COVINGTON & BURLING LLP

HOME > INTERNATIONAL > EUROPEAN UNION > BREXIT DEAL KEEPS EU-UK DATA FLOWS OPEN AS PARTIES PURSUE MUTUAL ADEQUACY

Brexit Deal Keeps EU-UK Data Flows Open as Parties Pursue Mutual Adequacy

By Dan Cooper and Kurt Wimmer on December 24, 2020

POSTED IN CROSS-BORDER TRANSFERS, EUROPEAN UNION, UNITED KINGDOM

On December 24th, with a year-end deadline and the holidays fast approaching, European Commission and United Kingdom (“UK”) officials **announced** they reached a deal on the EU-UK Trade and Cooperation Agreement (“Agreement”). Once formally adopted by the European Union (“EU”) institutions, the Agreement will govern the relationship between the EU and UK beginning on January 1, 2021, following the end of the Brexit transition period.

The Agreement is likely to avert a year-end scramble to secure cross-border data transfers between the EU and the UK. Although the final text has not yet been published, a **UK government summary** of the deal indicates that the parties agreed to allow for the continued free flow of personal data for up to six months to allow time for the EU and UK to adopt mutual “adequacy decisions,” in which each jurisdiction may recognize the other as offering adequate protection for transferred personal data. Absent these adequacy decisions (and the interim period established by the Agreement), organizations would need to consider implementing additional safeguards, such as standard contractual clauses, to transfer personal data between the EU and UK.

24.12.2020 официальные лица Европейской комиссии и Соединенного Королевства объявили, что достигли соглашения по соглашению о торговле и сотрудничестве между ЕС и Королевством. После официального принятия институтами ЕС Соглашение будет регулировать отношения между ЕС и Великобританией начиная с 01.01.2021.

Ключевые моменты Соглашения:

- стороны согласились разрешить непрерывный и свободный трансграничный обмен персональными данными до 01.07.2020, чтобы дать время ЕС и Великобритании для принятия решения о признании взаимной адекватности в сфере защиты персональных данных;
- предусмотрены обязательства ЕС и Великобритании поддерживать высокие стандарты защиты данных и воздерживаться от принятия требований по локализации данных;
- в государственных интересах предусмотрен обмен информацией о перемещающихся трансгранично пассажирах, о привлечении к уголовной ответственности, а также данными ДНК, отпечатками пальцев и регистрационными данными транспортных средств.



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 on data protection and Brexit implementation – what you need to do

Date 29 January 2020
Type Statement

The UK will leave the European Union on 31 January and enter a Brexit transition period.

During this period, which runs until the end of December 2020, it will be **business as usual** for data protection.

The GDPR will continue to apply. Businesses and organisations that process personal data should continue to follow our [existing guidance](#) for advice on their data protection obligations.

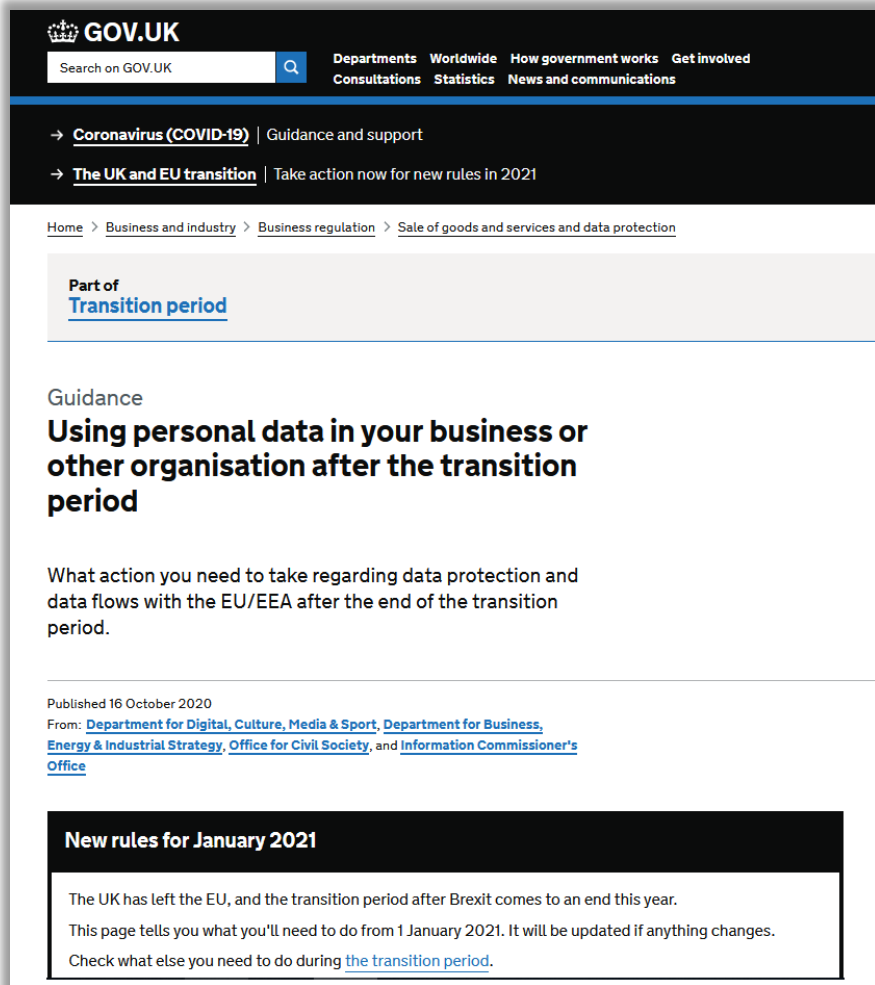
During the transition period, companies and organisations that offer goods or services to people in the EU do not need to appoint a European representative. We have updated our [Brexit FAQs](#) to reflect this advice. The ICO will continue to act as the lead supervisory authority for businesses and organisations operating in the UK.

It is not yet known what the data protection landscape will look like at the end of the transition period and we recognise that businesses and organisations will have concerns about the flow of personal data in future.

We will continue to monitor the situation and update our external guidance accordingly. Our [full suite of Brexit guidance and materials, to enable you to prepare for all scenarios, is available here](#).

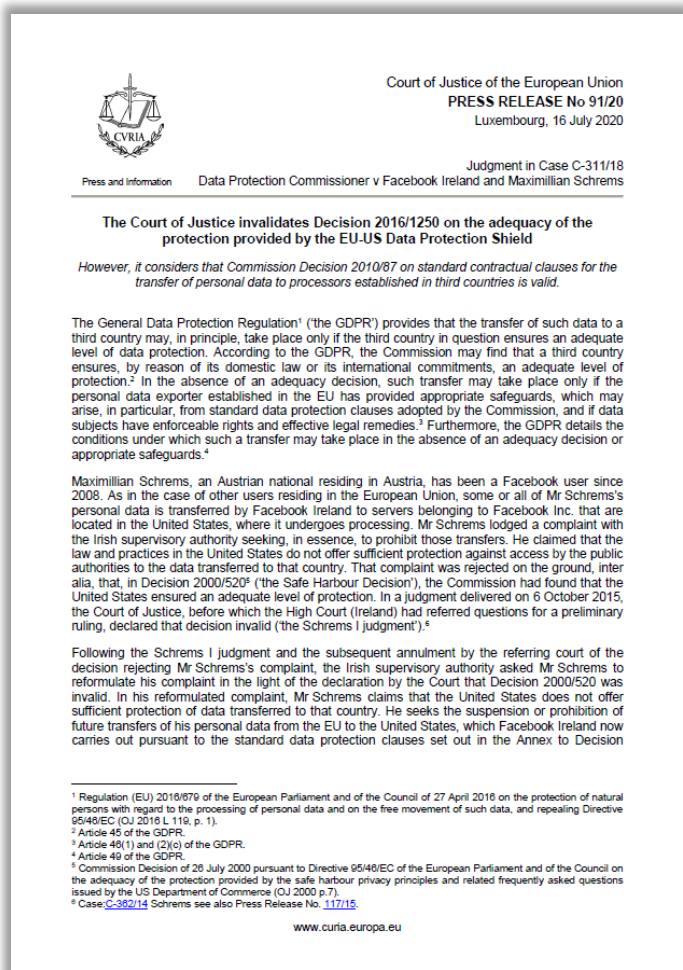
За несколько дней до выхода UK из состава ЕС, который произошел 31.01.2020, ICO обновил свое заявление об обмене данными между ЕС/ЕАСТ и Великобританией:

- В течение переходного периода (до 31.12.2020) GDPR будет сохранять действие на компании из UK;
- во время переходного периода компании, предлагающие товары и услуги субъектам в ЕС, не обязаны назначать представителя в ЕС;
- ICO продолжает быть ведущим регулятором для организаций из UK;
- сохраняется неопределённость по поводу сохранения статуса UK как страны, обеспечивающей адекватный уровень защиты, после окончания переходного периода.



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, Get involved, Consultations, Statistics, and News and communications. Below this, there are two main navigation items: 'Coronavirus (COVID-19) | Guidance and support' and 'The UK and EU transition | Take action now for new rules in 2021'. The breadcrumb trail reads: Home > Business and industry > Business regulation > Sale of goods and services and data protection. A banner indicates it is part of the 'Transition period'. The main heading is 'Guidance Using personal data in your business or other organisation after the transition period'. The sub-heading is '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.



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.

- 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. адекватности обеспечения защиты 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.

edpb
European Data Protection Board

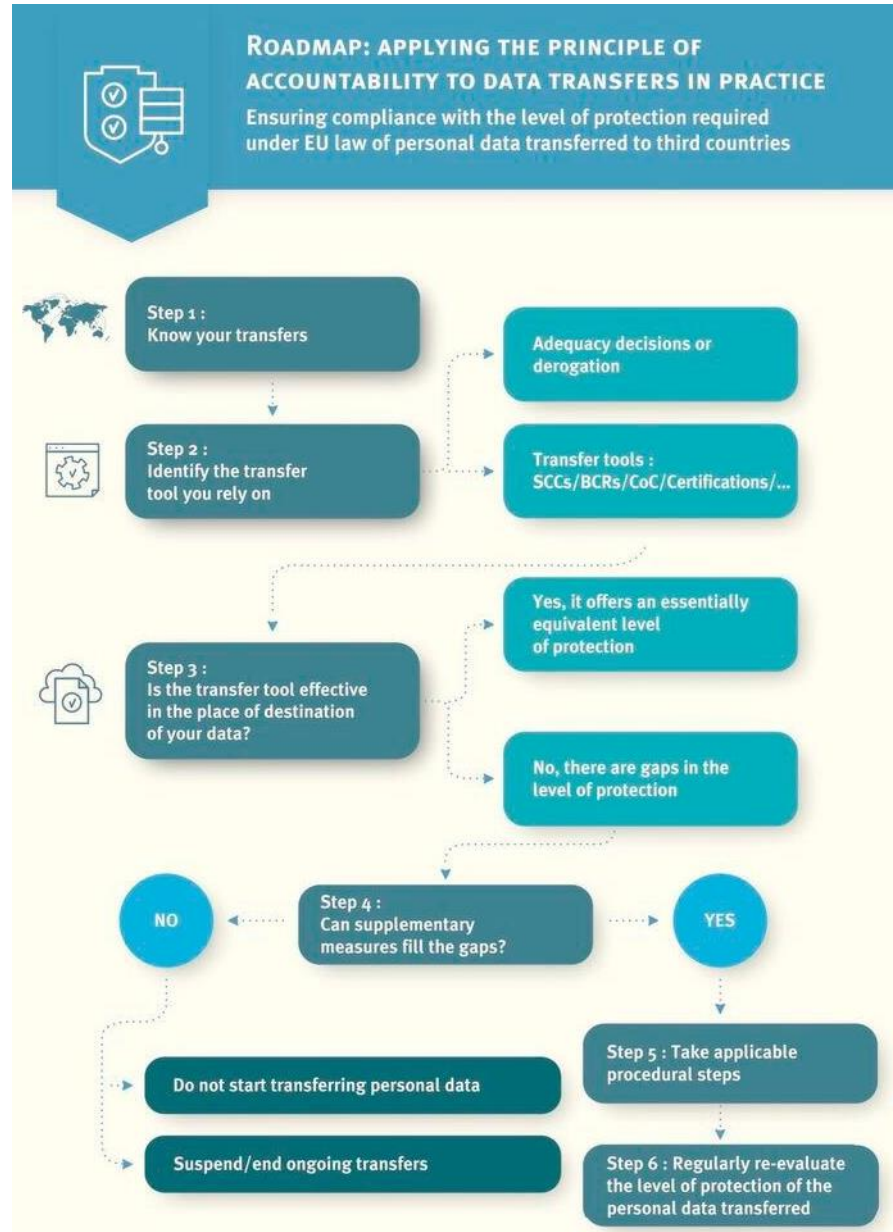
Recommendations

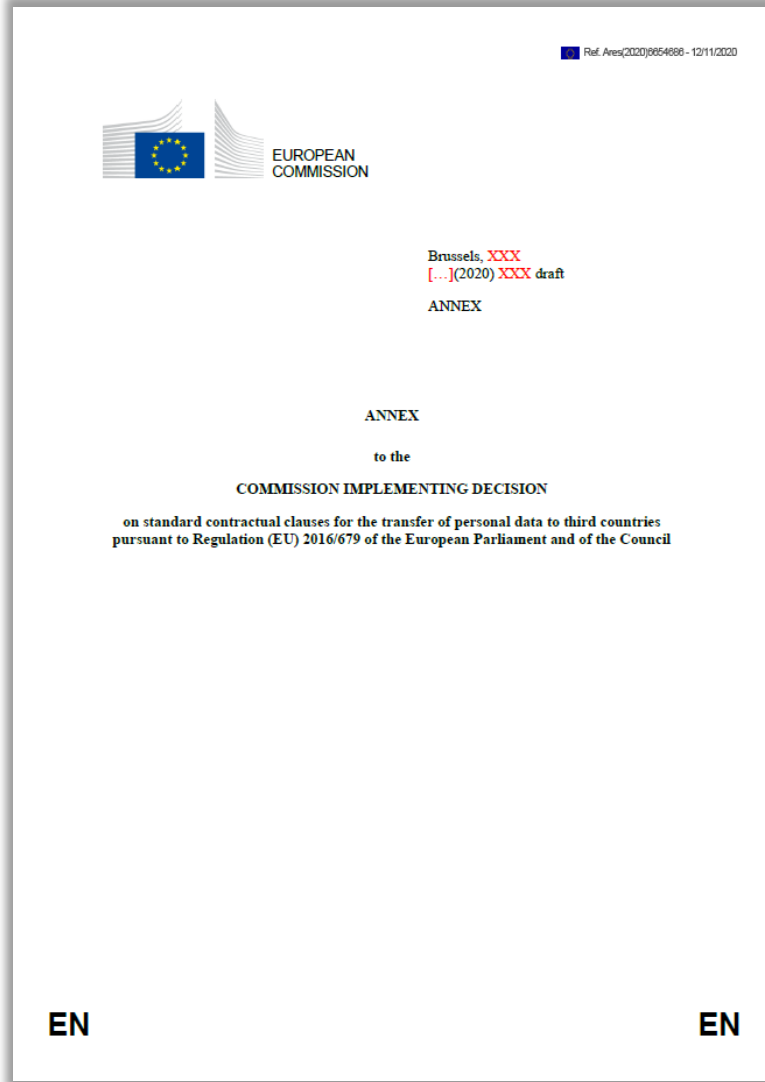
Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Adopted on 10 November 2020

Adopted - version for public consultations

1

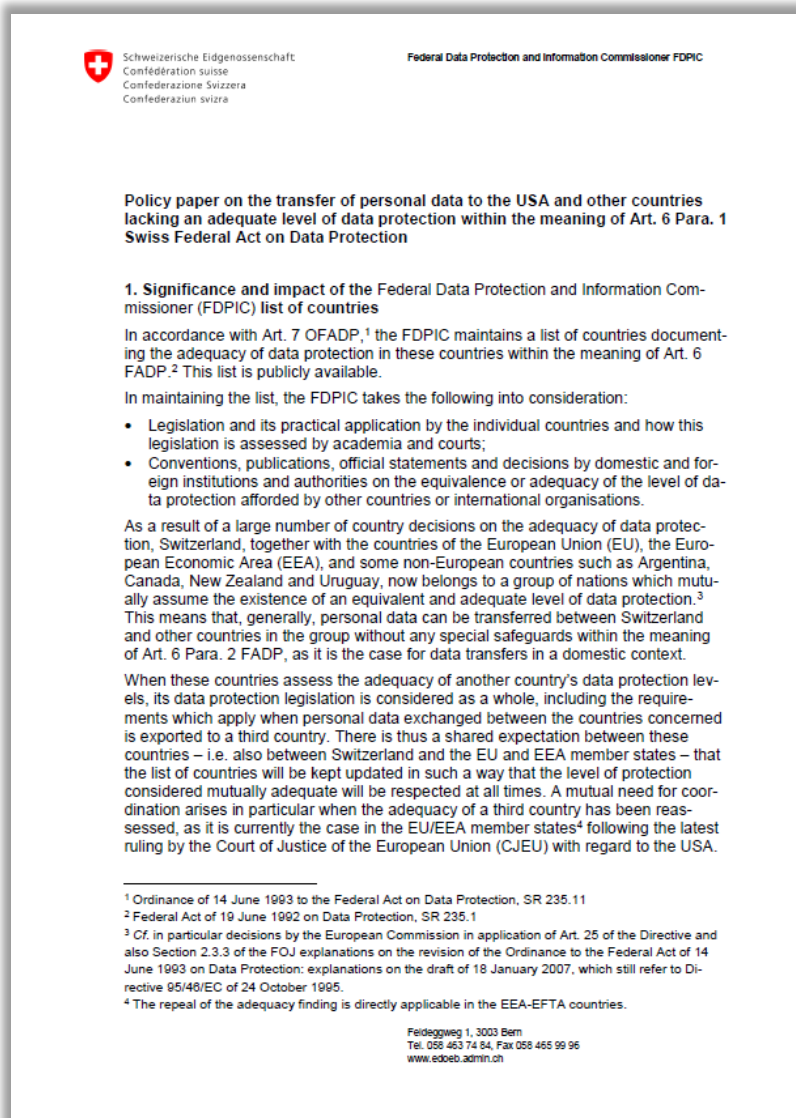




12.11.2020 Европейская Комиссия опубликовала проект новых Стандартный договорных условий для экспорта персональных данных из ЕС/ЕЭЗ в иностранные государства, обеспечивающие адекватную защиту прав субъектов данных. Также было предложено? Спустя 12 месяцев после утверждения новых SCC, признать не имеющими 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».



Швейцарский Федеральный комиссар по защите данных и информации (FDPIC) 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, FDPIC соглашается с критикой EDPB относительно доступа властей США к данным. Более того, FDPIC 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.

FDPIC 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.

Your path to **trusted** cloud services in Europe



Cloud Industry Unites to Create Global Standard for Transfer of Personal Data following 'Schrems II' ruling

Brussels, 15 September 2020 – The creators of the data protection market standard for cloud, the EU Cloud Code of Conduct, today announced work is underway on a proposed legal solution for the transfer of personal data outside the EU. Once approved by data protection authorities, the solution could be an alternative to the recently annulled EU-U.S. Privacy Shield, previously relied on by thousands of businesses who now face disruption and uncertainty when transferring EU citizens' data across the Atlantic.

The EU Data Protection Code of Conduct for Cloud Service Providers ("EU Cloud Code of Conduct") defines clear requirements for Cloud Service Providers acting as "processors" under the General Data Protection Regulation (GDPR) and is adopted broadly by the cloud market. While the official approval of the current Code by the European Data Protection Board (EDPB), comprised of national Data Protection Authorities (DPAs), is pending, the EU Cloud Code of Conduct General Assembly today announced in a virtual press conference the creation of a new module to the Code for transferring personal data outside of the EU.

The announcement comes only weeks after the recent European Court of Justice's so-called "Schrems II" ruling which invalidated the data exchange mechanism between the US and the EU (Privacy Shield). The ruling also imposed strict obligations on companies that rely on transfers of personal data to non-EU countries by Standard Contractual Clauses.

The EU Cloud Code of Conduct General Assembly invites interested Cloud Service Providers (CSPs) and cloud-users to join the initiative and to contribute to the development of the module, thereby shaping the future legal basis to transfer EU citizen's personal data to third countries around the world.

EU Cloud Code of Conduct
c/o SCOPÉ Europe b.v.b.a./s.p.r.l.
Rue de la Science 34
1040 Brussels, Belgium

info@eucoc.eu
+32 2 809 5319
<https://eucoc.cloud>

1 | 3

Европейская ассоциация провайдеров облачных услуг предлагают использовать, после его определенной доработки, Кодекс поведения ЕС в отношении облачных вычислений (EU Cloud Code of Conduct) в качестве альтернативы соглашению EU-U.S. Privacy Shield, аннулированному Европейским судом в рамках решения Schrems II. Указанный кодекс охватывает весь спектр облачных сервисов (SaaS, PaaS, IaaS) и в настоящее время ожидает утверждения со стороны Европейского совета по защите данных (EDPB).

















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 (S)igned; (R)atified; (E)ntered into force	CoE 108+ (223) Data Protection (S)igned; (R)atified; (E)ntered into force
+ Switzerland	✓ See here	✓	✓	✓	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	✓ See here	✗	✗	✓ See here or here		
+ Kuwait	✗	✗	✗	✗		
+ Oman	✗	✗	✗	✗		
+ Qatar	✗	✗	✗	✓ See here or here		
+ Serbia	✗ Potential future candidate (p. 52) for adequacy?	✗	✗	✓	S, R, E: 01/01/2006	S, R
+ Russian Federation	✗	✗	✗	✓	S, R, E: 01/09/2013	S

Рекомендации, руководства и практические пособия



Руководства, рекомендации, лучшие практики в области выполнения требований GDPR от Европейского совета по защите данных (European Data Protection Board):

1. [Guidelines 10/2020 on restrictions under Article 23 GDPR - version for public consultation](#)
2. [Recommendations 02/2020 on the European Essential Guarantees for surveillance measures](#)
3. [Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - version for public consultation](#)
4. [Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 - version for public consultation](#)
5. [Guidelines 08/2020 on the targeting of social media users - version for public consultation](#)
6. [Guidelines 07/2020 on the concepts of controller and processor in the GDPR - version for public consultation](#)
7. [Guidelines 05/2020 on consent under Regulation 2016/679](#)
8. [Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak](#)
9. [Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak](#)
10. [Guidelines 2/2020 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 - version adopted after public consultation](#)
11. [Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications - version for public consultation](#)
12. [Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR \(part 1\)](#)
13. [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#)
14. [Guidelines 3/2019 on processing of personal data through video devices](#)
15. [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\)](#)
16. [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 - version for public consultation](#)
17. [EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation](#)
18. [EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation \(2016/679\) - version adopted after public consultation](#)
19. [EDPB Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\)](#)
20. [EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679](#)
21. [EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation](#)

Значимые письма Европейского совета по защите данных о выполнении требований GDPR:

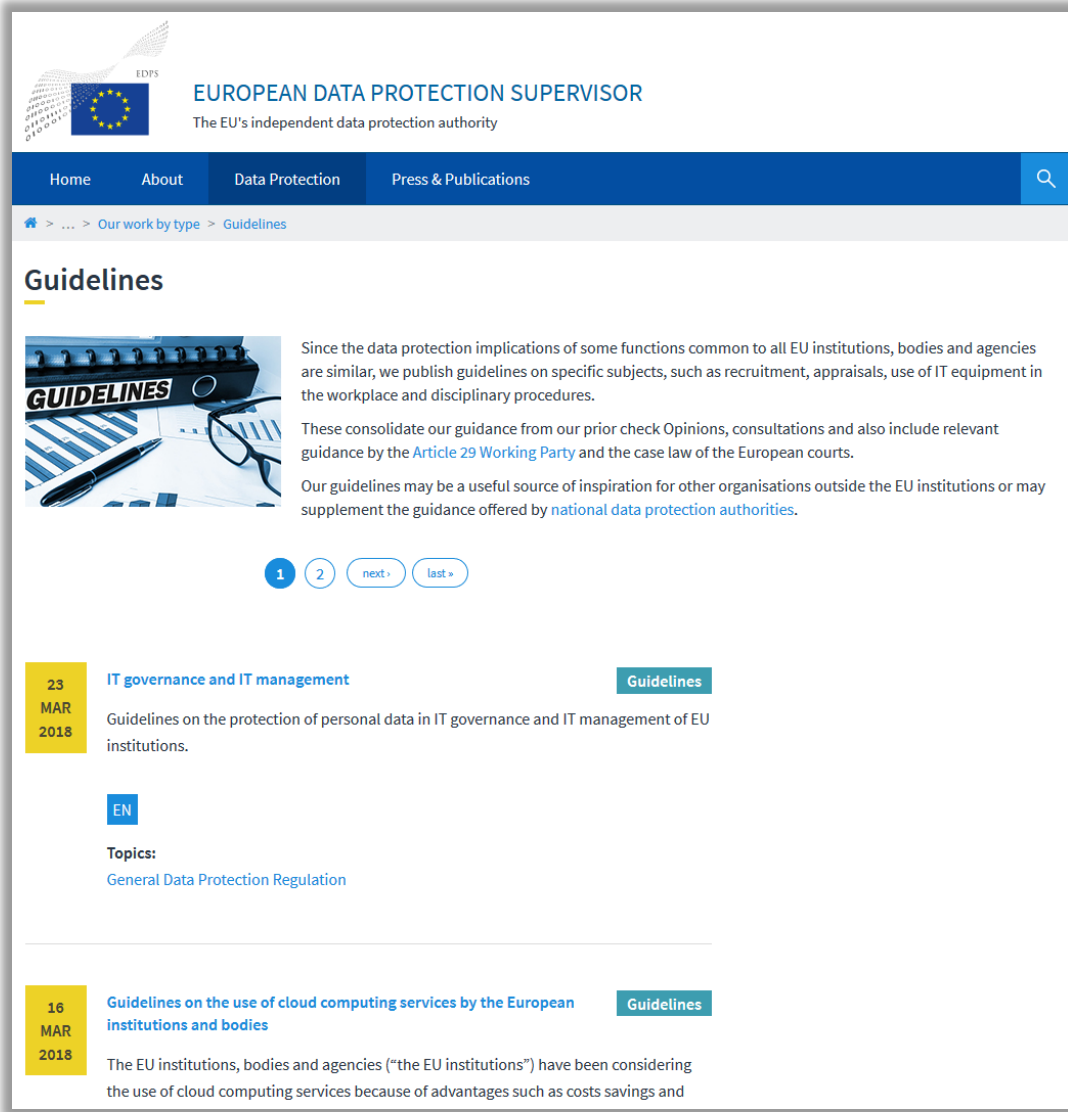
1. [Statement on the processing of personal data in the context of the COVID-19 outbreak — 19/03/2020](#)
2. [EDPB Response to the MEP Sophie in't Veld's letter on unfair algorithms](#)

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 Personal data breach notification under Regulation 2016/679, WP250 rev.01](#)
5. [Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01](#)
6. [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](#)
7. [Guidelines on Data Protection Officers \('DPO'\), WP243 rev.01](#)
8. [Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01](#)
9. [Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30\(5\) GDPR](#)
10. [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](#)
11. [Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264](#)
12. [Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265](#)
13. [Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01](#)
14. [Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01](#)
15. [Adequacy Referential, WP 254 rev.01](#)
16. [Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253](#)

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](#)




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.


COUNCIL OF EUROPE
Data Protection

Home
Convention 108 and Protocols ▾
Activities ▾
Documentation ▾
Data Protection Commissioner
Data Protection Day

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 ICDPPC 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 ⤵

2016 ⤵

2015 ⤵

2014 ⤵


2013 ⤵

2012 ⤵

2011 ⤵

2010 ⤵

2009 ⤵

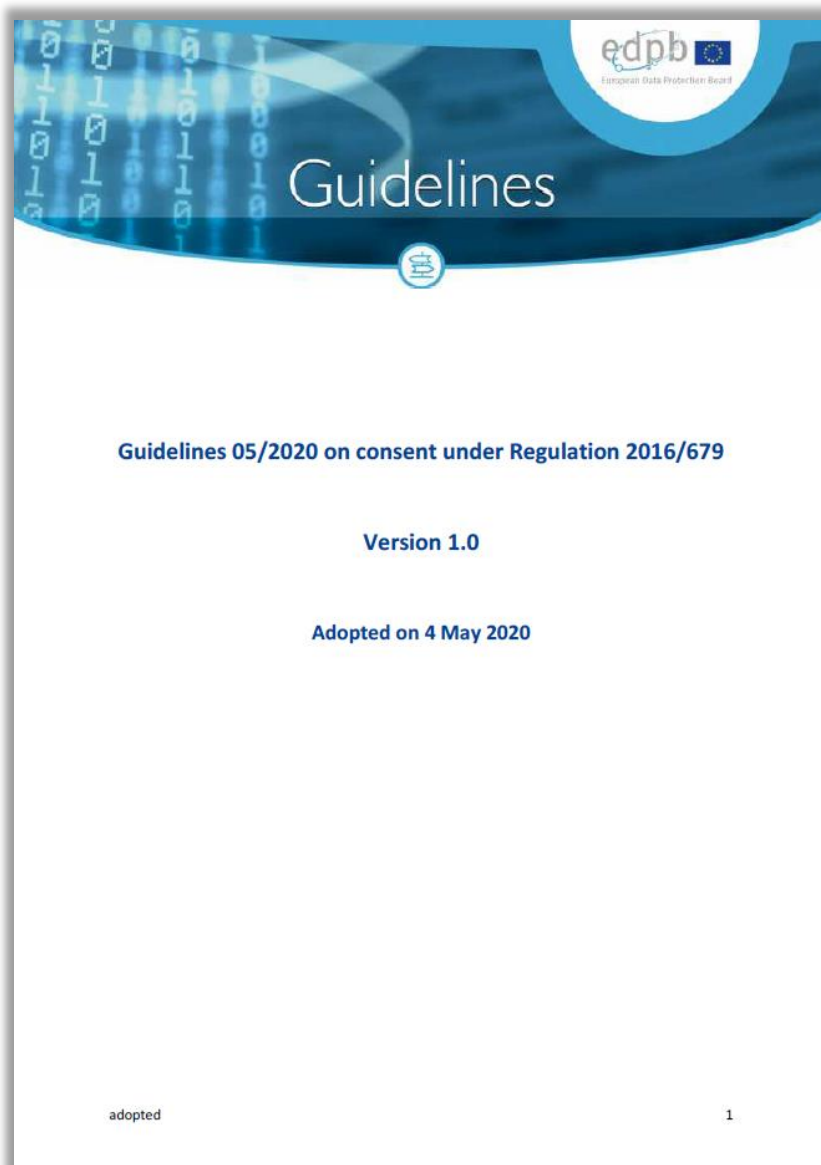


www.coe.int/dataprotection

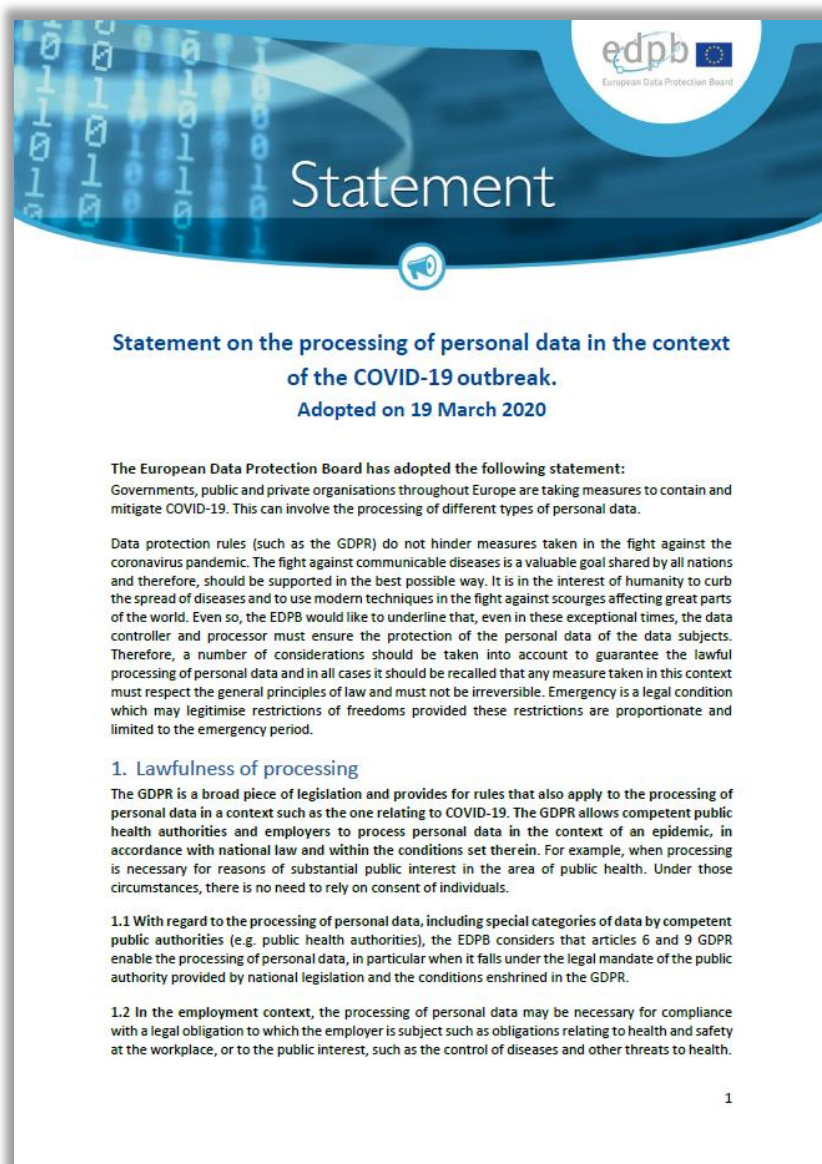
ECHR Factsheets

- 📄 [Personal data protection](#)
- 📄 [New technologies](#)

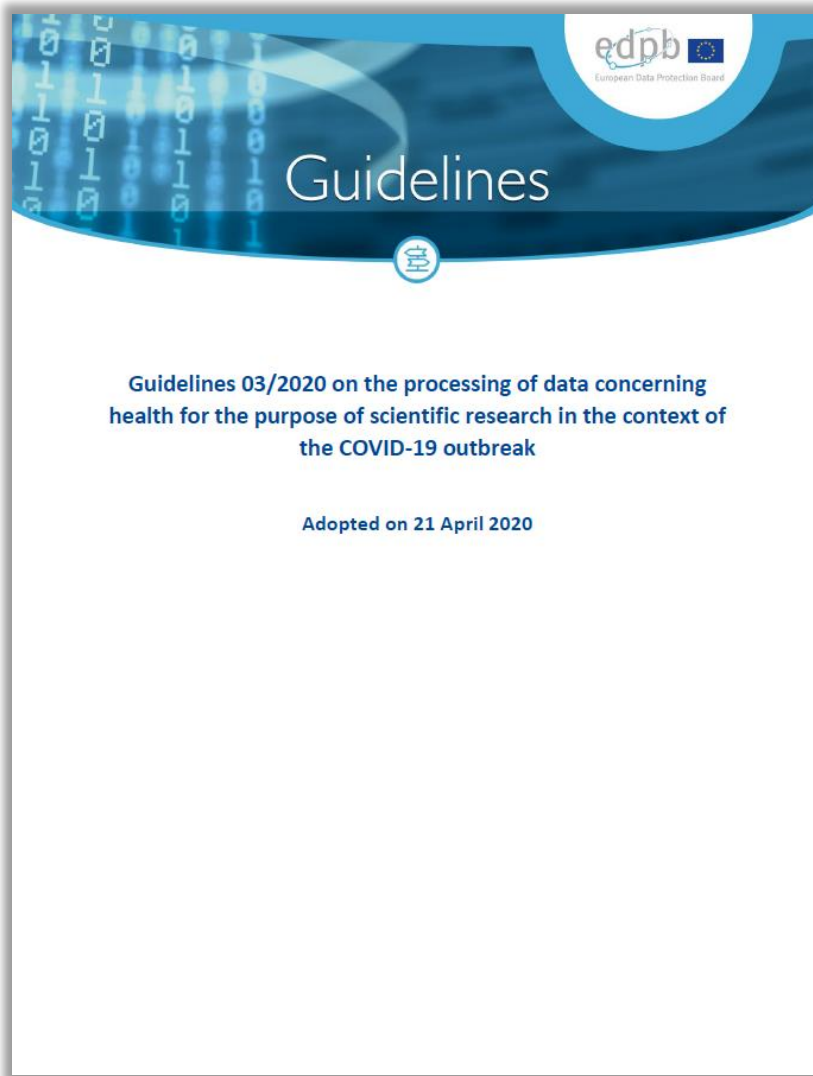
✉ [Contact us](#)



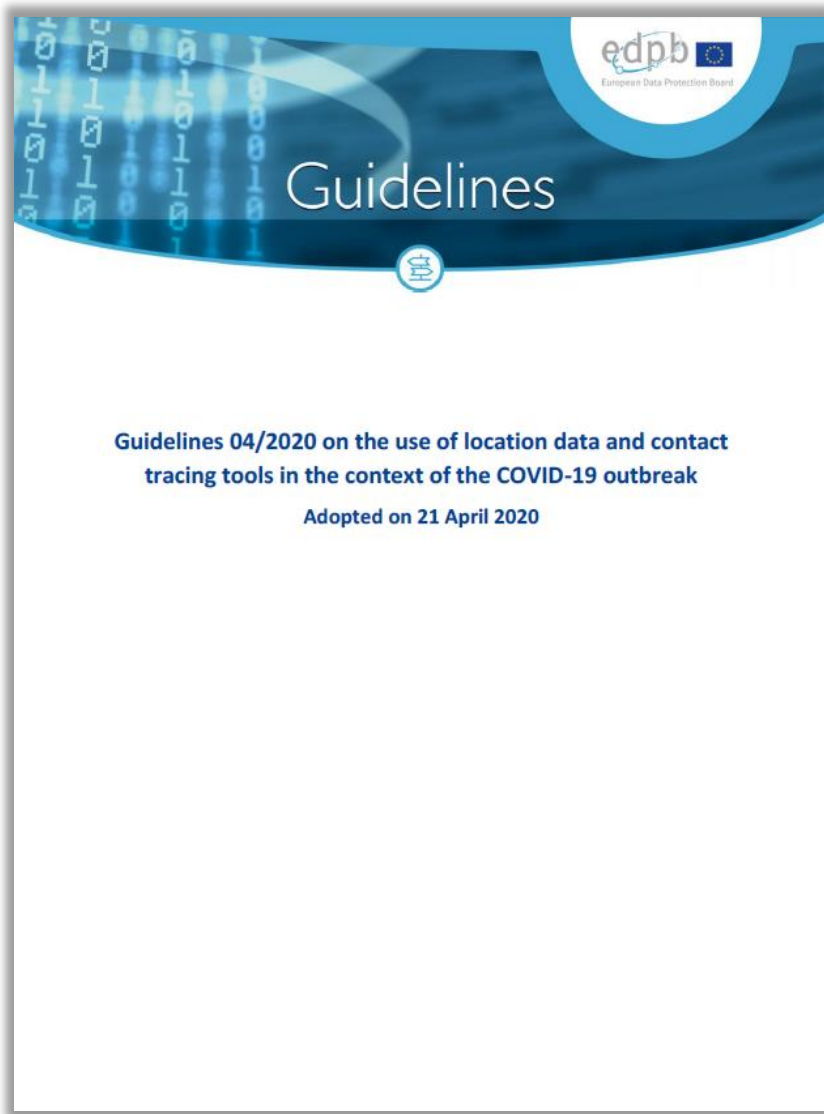
0	Preface.....
1	Introduction.....
2	Consent in Article 4(11) of the GDPR
3	Elements of valid consent
3.1	Free / freely given
3.1.1	Imbalance of power.....
3.1.2	Conditionality
3.1.3	Granularity.....
3.1.4	Detriment
3.2	Specific.....
3.3	Informed.....
3.3.1	Minimum content requirements for consent to 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



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.



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.



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).





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	• Policies and procedures
• Training and awareness	• Individuals' rights
• Transparency	• Records of processing and lawful basis
• Contracts and data sharing	• Risks and data protection impact assessments
• Records management and security	• 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

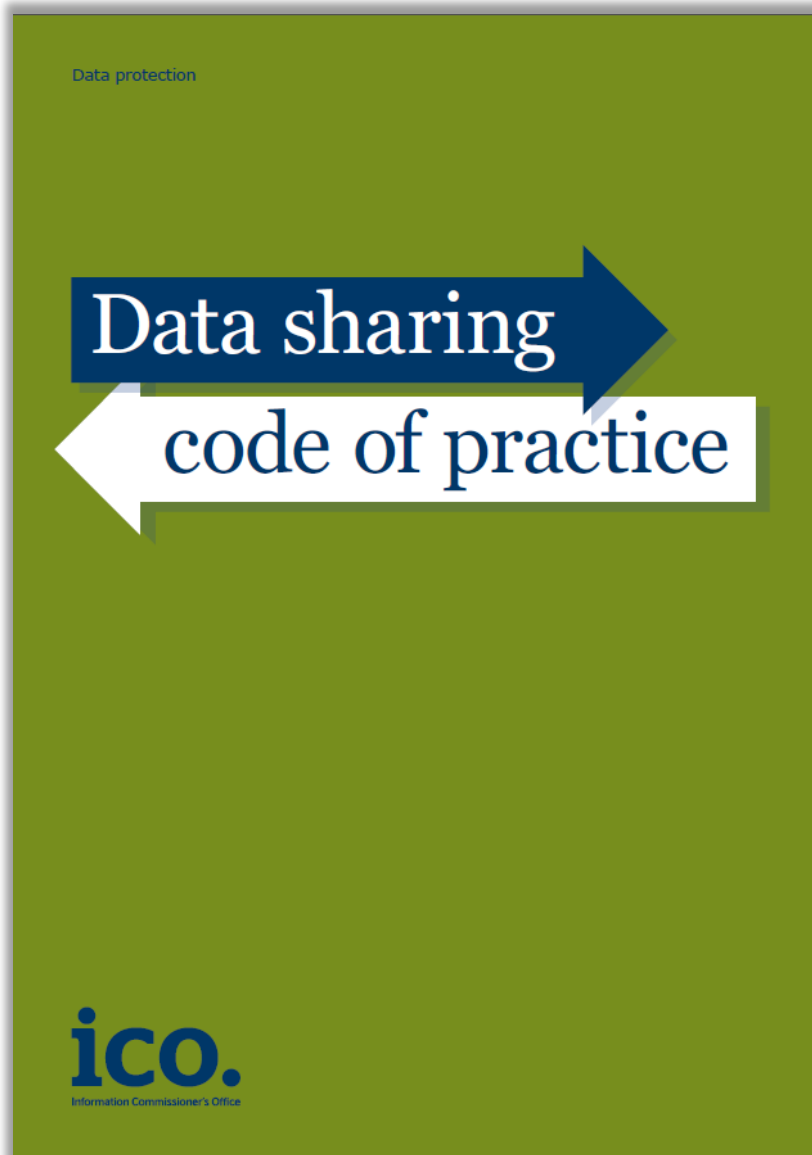
Reviewing and monitoring

External audit or compliance check

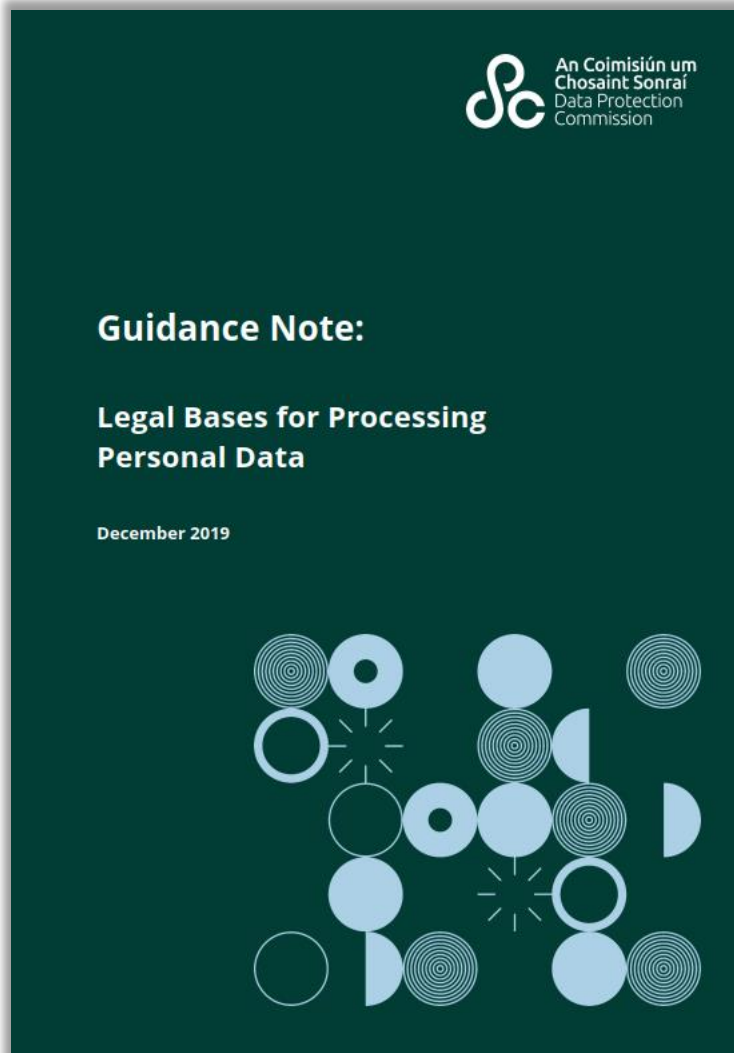
Internal audit programme

Performance and compliance information

Use of management information

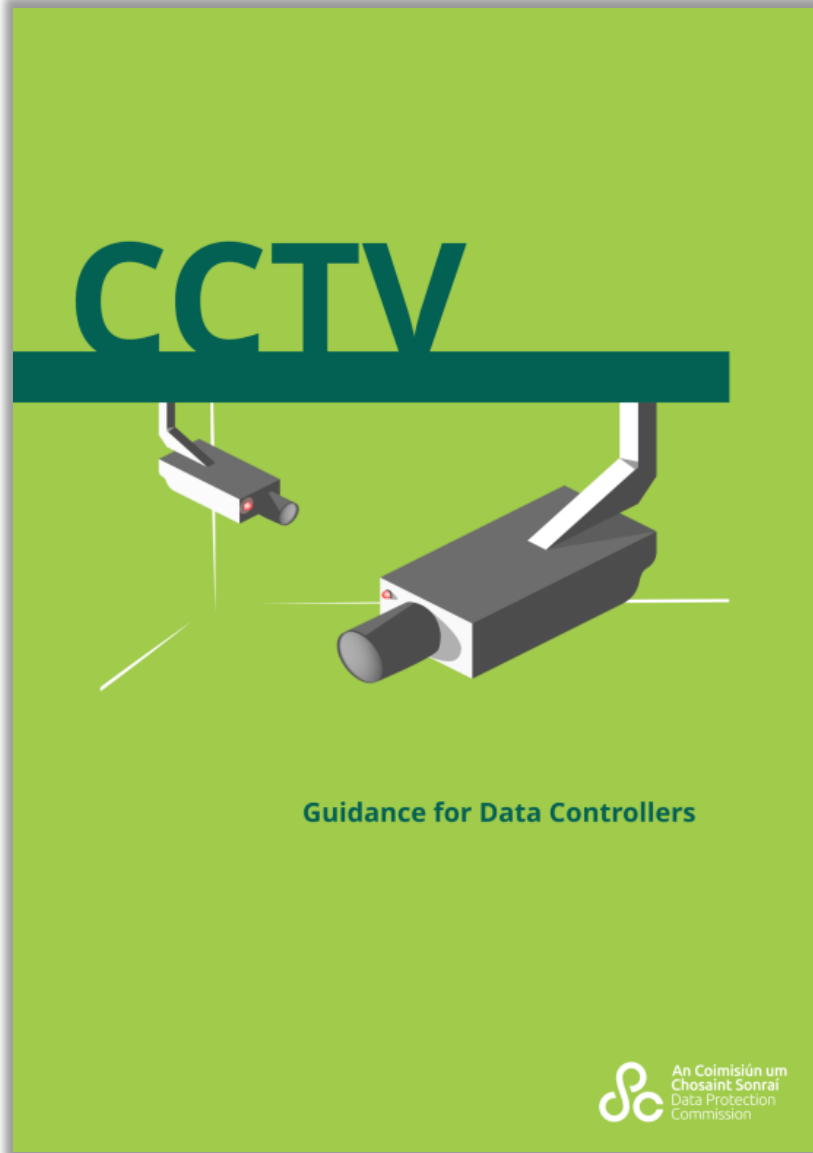


Британский надзорный орган ICO (Information Commissioner's Office), в соответствии со ст.121 Data Protection Act 2018, опубликовал для проведения публичных консультаций проект обновленного кодекса поведения по предоставлению данных - Data Sharing Code of Practice - документ, который применяет все правила GDPR для ситуаций, когда компания делится персональными данными с кем-либо еще.

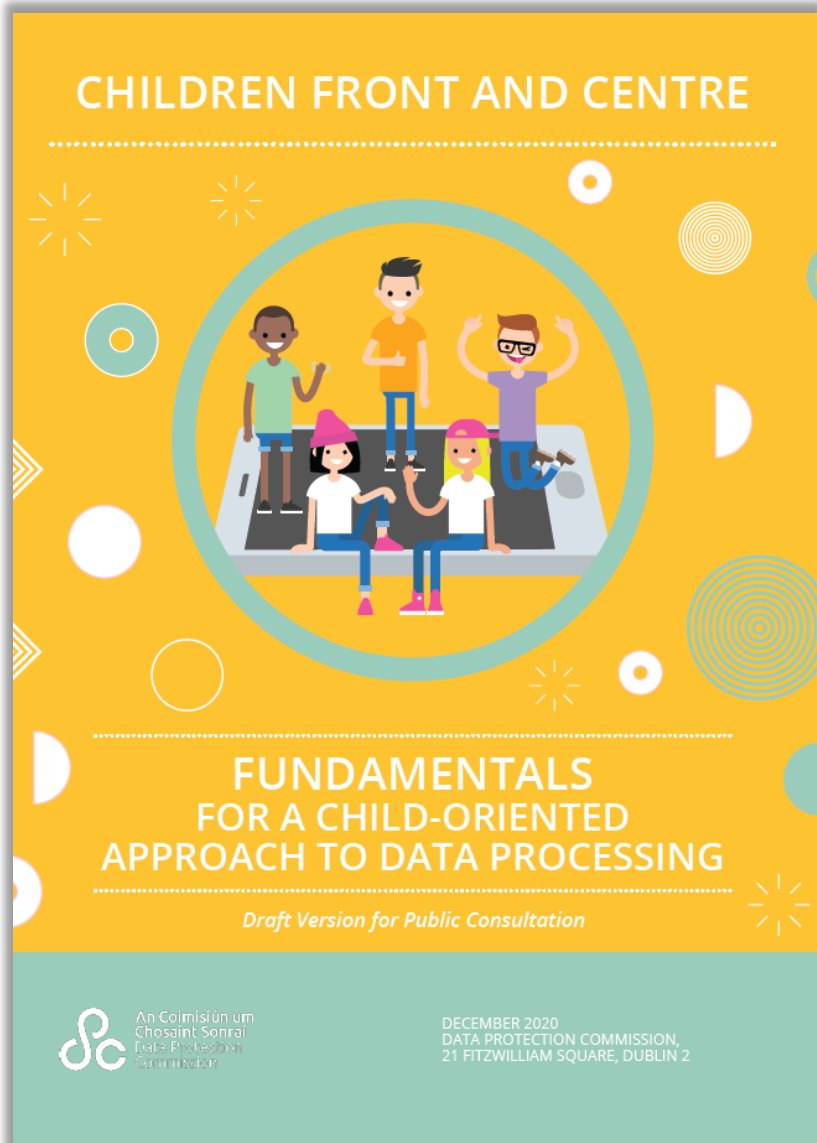


Ирландский надзорный орган Data Protection Commission в декабре 2019 года опубликовал руководство для контролеров по определению правильной правовой основы для той или иной обработки персональных данных и обязательств, которые соответствуют этой правовой основе.


	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	✓	✓	✓	✓	✗	✓






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	



Ирландская Комиссия по защите данных (Data Protection Commission) опубликовала для публичного обсуждения (до **31.03.2021**) 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.




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.



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




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) 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 мая 2020 г. 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.



The screenshot shows the website of the Swedish Data Protection Authority (Datainspektionen). The page title is "Behandling av personuppgifter i arbetslivet". Below the title is a subtitle: "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, arbetssökande, fackförbund och branschorganisationer." The page features a grid of 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".

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 сотрудниках, какие правила следует соблюдать при приеме на работу, каковы ограничения по контролю и мониторингу сотрудников, а также по обработке биометрии.



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

@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.

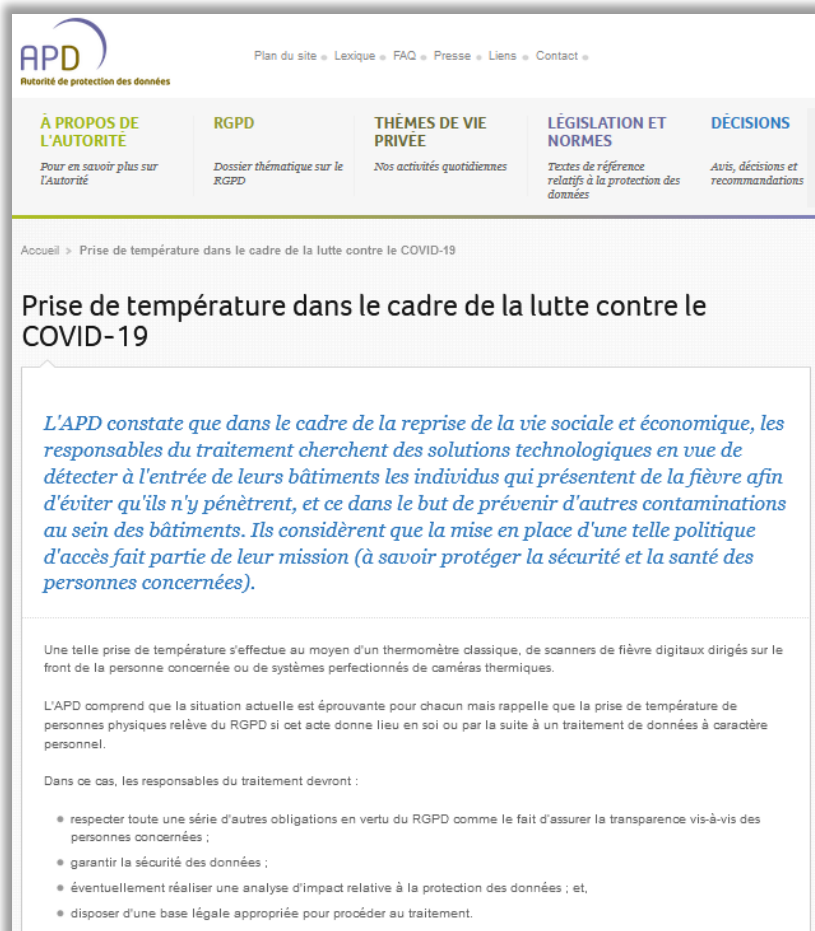
Assessing **proportionality**:

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.).



APD
Autorité de protection des données

Plan du site » Lexique » 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	LÉGISLATION ET NORMES Textes de référence relatifs à la protection des données	DÉCISIONS Avis, 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.

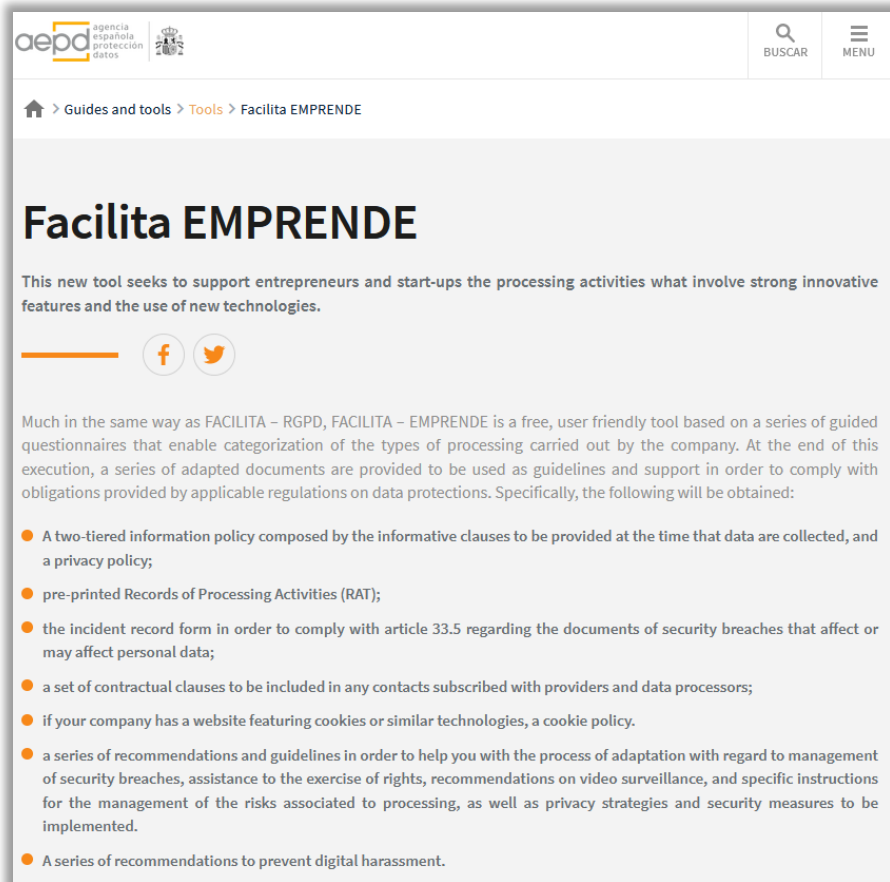
L'APD comprend que la situation actuelle est éprouvante pour chacun mais rappelle que la prise de température de personnes physiques relève du RGPD si cet acte donne lieu en soi ou par la suite à un traitement de données à caractère personnel.


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 5 июня 2020 года 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.







 BUSCAR
  MENU

[Home](#) > [Guides and tools](#) > [Tools](#) > [Facilita EMPRENDE](#)

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.

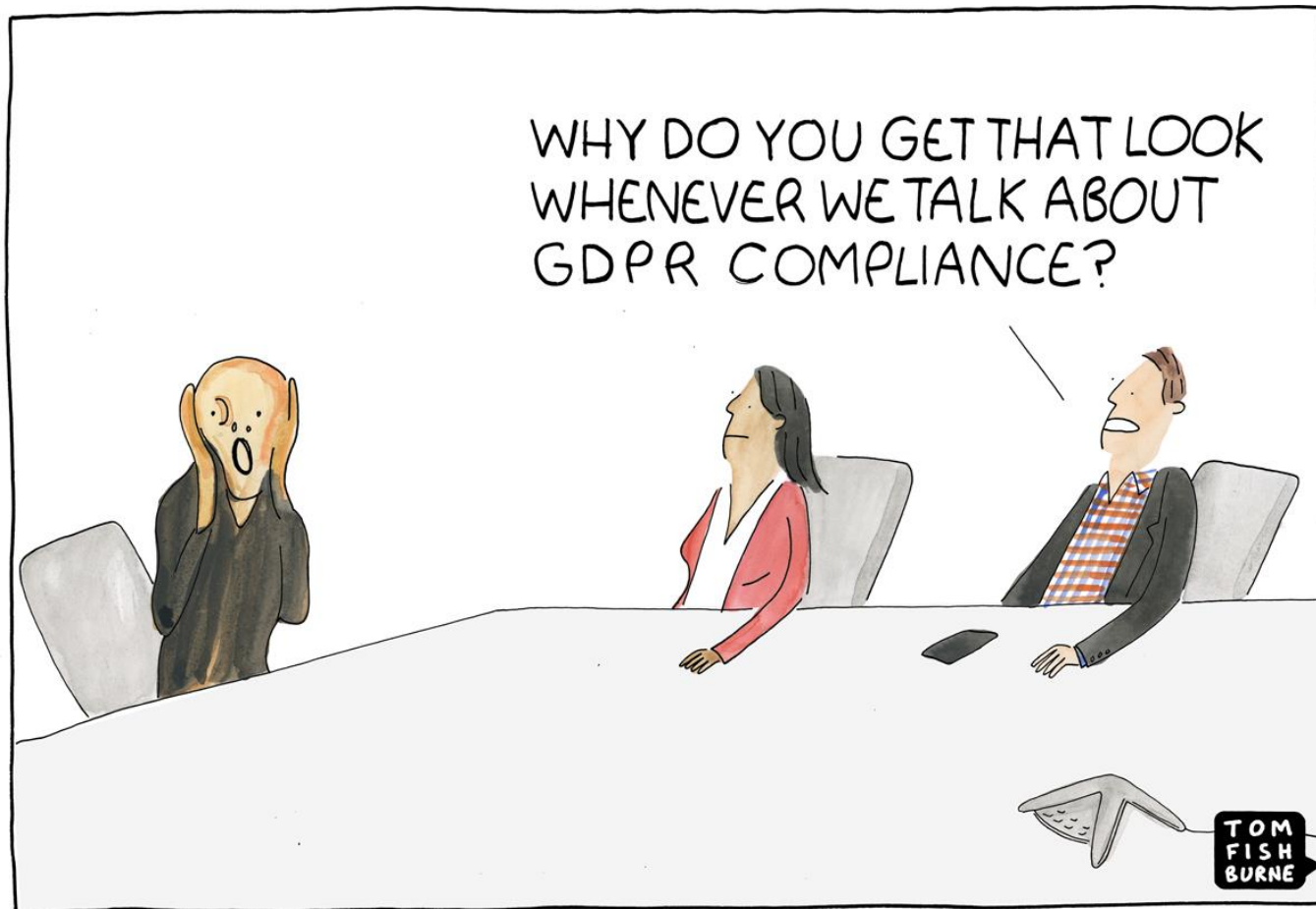



Much in the same way as FACILITA – RGPD, FACILITA – EMPRENDE is a free, user friendly tool based on a series of guided questionnaires that enable categorization of the types of processing carried out by the company. At the end of this execution, a series of adapted documents are provided to be used as 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.

Вспомогательная информация от коммерческих и некоммерческих организаций





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 projects. 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

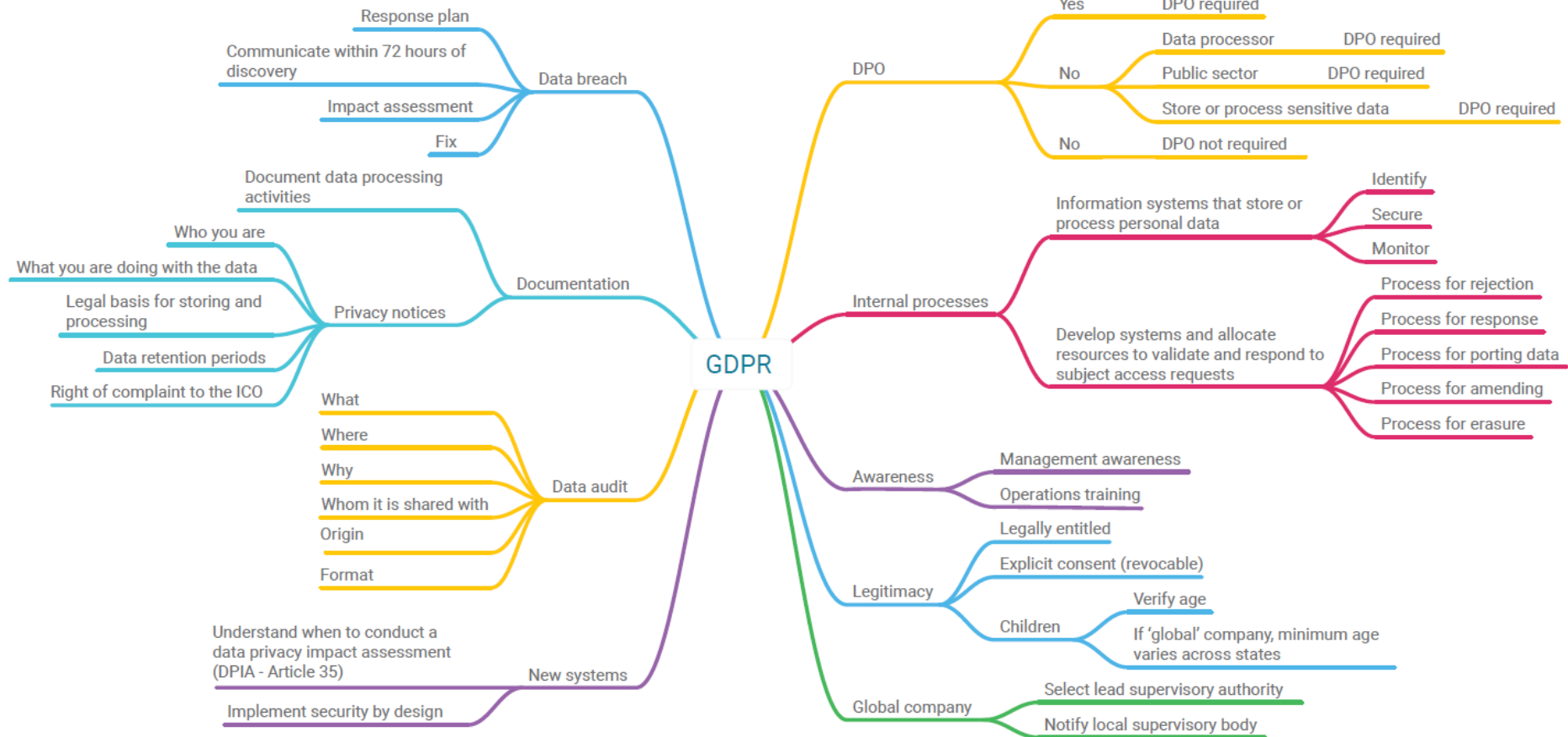
Although the GDPR does not contain many provisions on processing personal data of minor's, most DPAs recommend to take extra care when dealing with data from children. Organisations are recommended to put in place specific safeguards where possible. Also compliance with the minimum age for consent in 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.

Key GDPR Domains and Requirements



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	

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
Consent Art. 6(1)(a)	Yes. Consent can be withdrawn. Art. 7(3)	Yes. Withdrawal can trigger right. Art. 17(1)(b)	Yes. Art. 20(1)(a)	Yes. Explicit consent allows automated decision making. Art. 22(2)(c)	Yes. Must refer to withdrawal right. Art. 13(2)(c) Art. 14(2)(d)	No.	No.	Restrictions on children consenting online. Art. 8
Contract Art. 6(1)(b)	No.	No.	Yes. Art. 20(1)(a)	Yes. Allows automated decision making. Art. 22(2)(a)	No.	No.	No.	No.
Legal obligation Art. 6(1)(c)	No.	No, and may be a defence to the exercise of right. Art. 17(3)(b)	No.	Yes. Allows automated decision making. Art. 22(2)(b)	No.	Yes. Art. 55(2)	Possibly. Art. 35(10)	No.
Vital interests Art. 6(1)(d)	No.	No.	No.	Yes. Individuals have right not to be subject to this. Art. 22	No.	No.	No.	No.
Public functions Art. 6(1)(e)	Yes. Right to object applies. Art. 21(1)	No, and may be a defence to the exercise of right. Art. 17(3)(b)	No. See express exclusion in Art. 20(3)	Yes. Individuals have right not to be subject to this. Art. 22	Yes. Must refer to right to object. Art. 21(4)	Yes. Art. 55(2)	Possibly. Art. 35(10)	No.
Legitimate interests Art. 6(1)(f)	Yes. Right to object applies. Art. 21(1)	Possibly. Art. 17(1)(c)	No.	Yes. Individuals have right not to be subject to this. Art. 22	Yes. Must refer to legitimate interests and right to object. Art. 13(1)(d) 14(2)(b) & 21(4)	No.	No.	Cannot be used by public authorities. Can be difficult to use with children. Art. 6(1)(f)

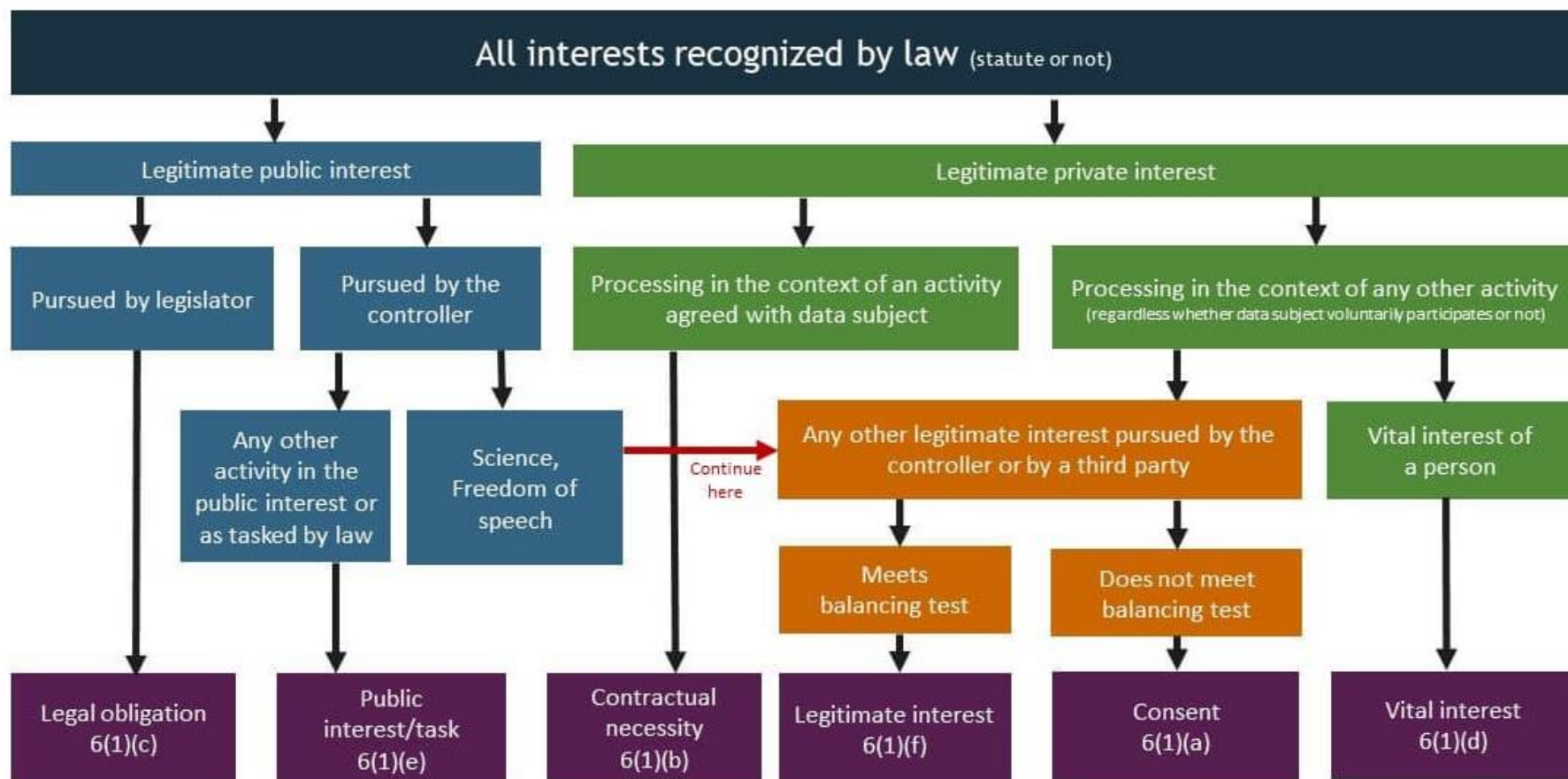
- Для веб-разработчиков: [руководство по приватности для браузеров](#) от команды разработчиков Chrome
- Для разработчиков приложений: [руководство по защите конфиденциальности пользователей](#), составленное Atlassian для разработчиков приложений, в котором описаны требования GDPR, а также обязанности 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

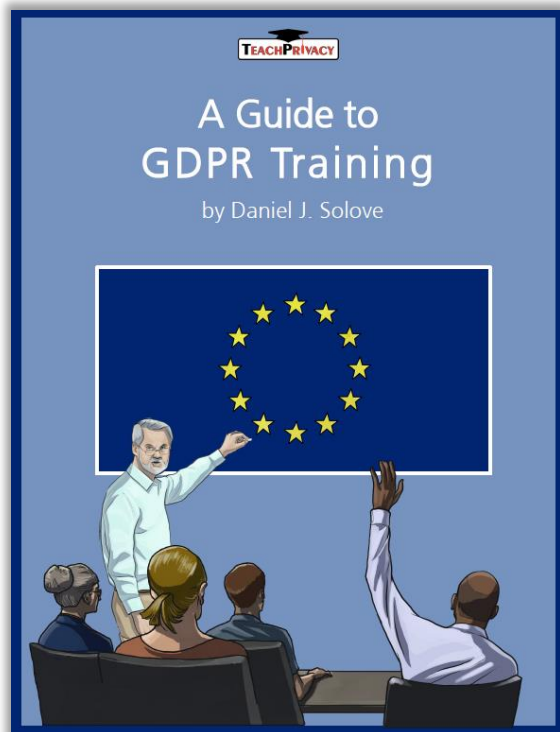


The screenshot shows a webpage from SmartRecruiters. The navigation bar at the top includes 'SmartRecruiters' and four menu items: 'PRODUCT', 'PLATFORM', 'HIRING SUCCESS', and 'COMPANY'. The main heading is 'GDPR and Recruitment Frequently Asked Questions'. Below the heading is a paragraph: 'The [General Data Protection Regulation \(GDPR\)](#) will greatly impact the way companies recruit globally. We have answered some of the most urgent questions recruiters have about what this means for them and what they need to do now to prepare.' A green button labeled 'READ FAQs' is positioned over the image. The background of the page features several European Union flags flying in front of a modern glass building.

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.

Choosing the right legal basis in the 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.

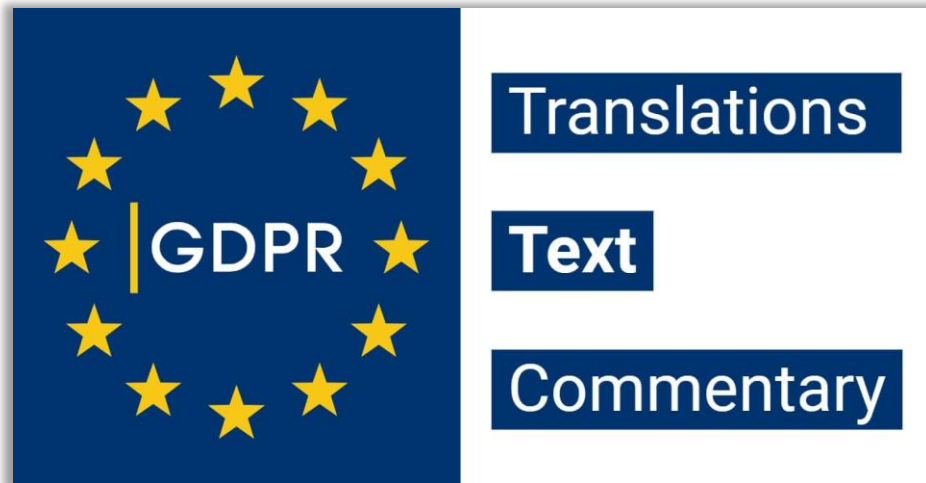
People don't need to know each particular definition — otherwise, their heads would spin. The key goal here is to get people to understand that a lot of data that they might not think is personal data in fact can be personal data. Data that alone is not identified to a particular person can be combined 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.

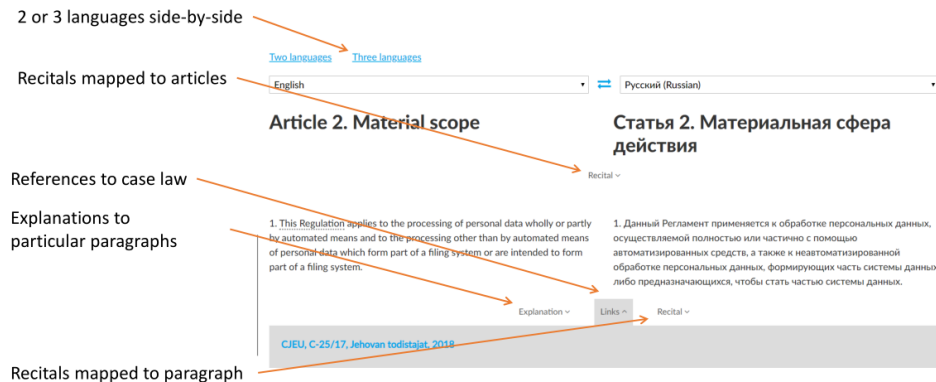


Responsibilities

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.




Features



Перевод подготовлен командой практиков, ежедневно работающих с GDPR. Работа велась под руководством Certified Information Privacy Professional (Europe) и Certified Data Privacy Manager Сергея Воронкевича.


- ✓ Выбрана корректная и наиболее приближенная к первоисточнику терминология в переводе:
 - процессор вместо обработчика;
 - контролер вместо контролера;
 - легитимный интерес вместо законного;
 - ограничение целью вместо ограничения цели.
- ✓ Текст приведен в табличный вид, где рядом с переводом показывается оригинал на официальном языке ЕС. Имеется переключатель между множеством языков. Можно выводить и три языка.
- ✓ Под статьями или параграфами есть ссылки на судебные прецеденты и Guidelines надзорных органов (включая самые свежие вроде на тему data protection by design).
- ✓ Размещены комментарии и объяснения.
- ✓ Всплывающие подсказки с определениями терминов из статьи 4.
- ✓ Mapping преамбул не только к статьям, но и отдельным параграфам внутри статей. Вы можете прочитать нужную преамбулу, не покидая страницу.






GDPRhub.eu

[Start Page](#)
[Random Page](#)
[@GDPRhub](#)

GDPRtoday

 [Get free updates!](#)

Start contributing!

 [Edit a page...](#)
 [Add a decision...](#)
 [Send a hint](#)

[noyb.eu](#)

[noyb.eu](#)
[Support us!](#)

Wiki tools

[Special pages](#)
[Cite this page](#)

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.

Data Protection (Privacy) by Design and by Default



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.

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.



Privacy and Data Protection by Design – from policy to engineering

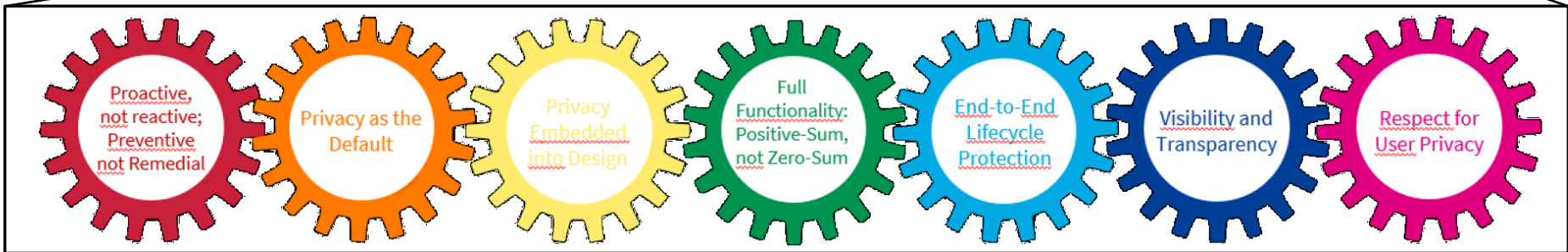
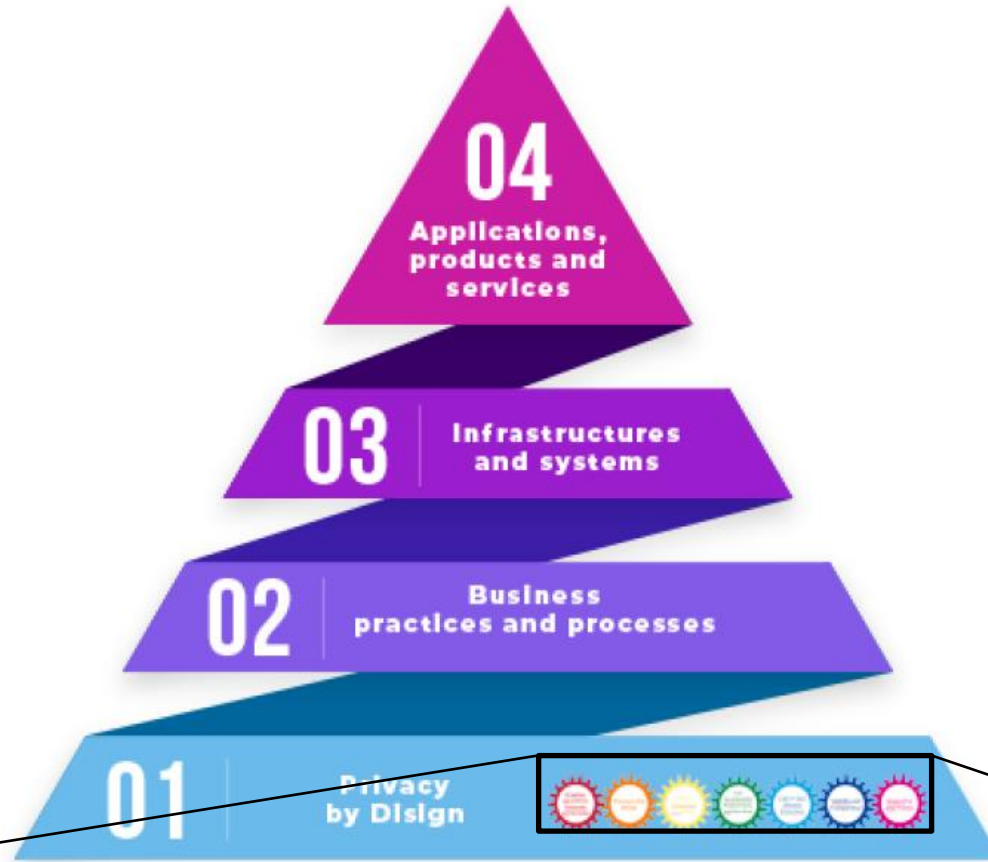
December 2014

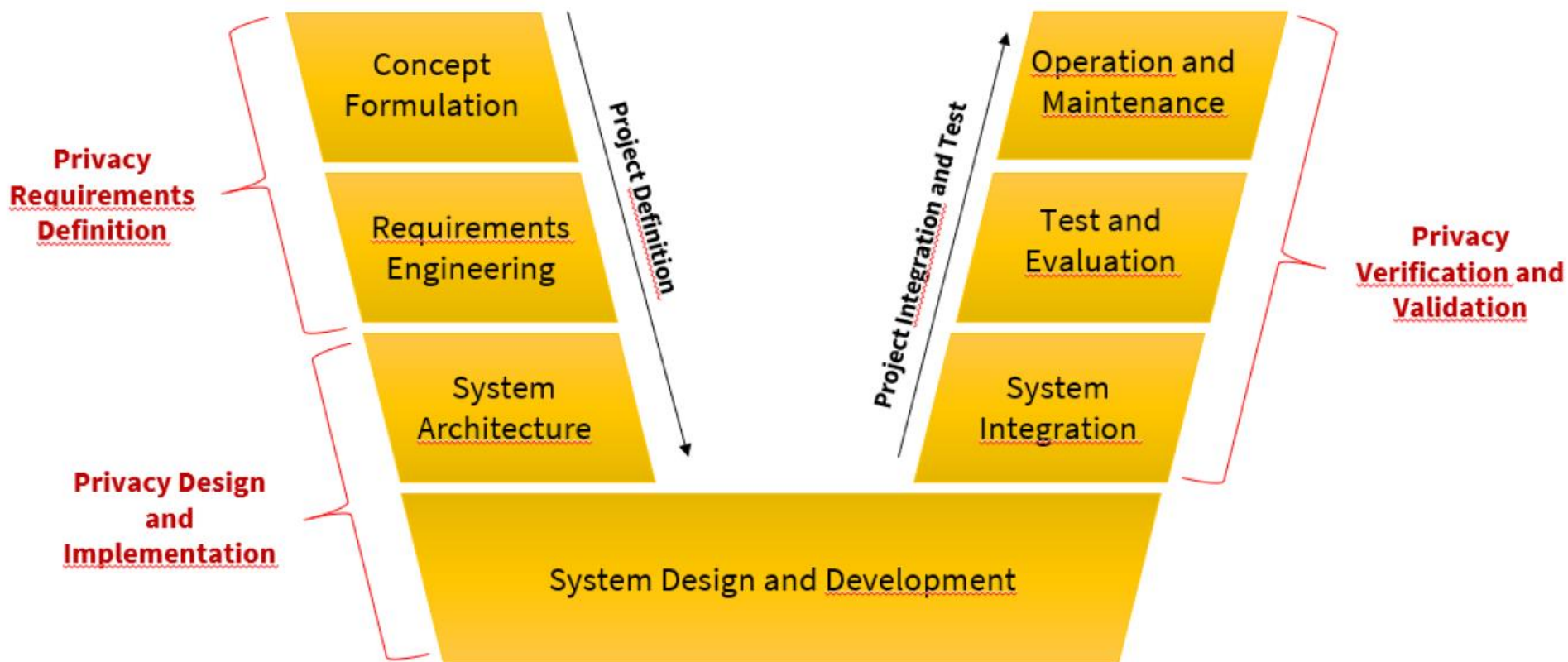


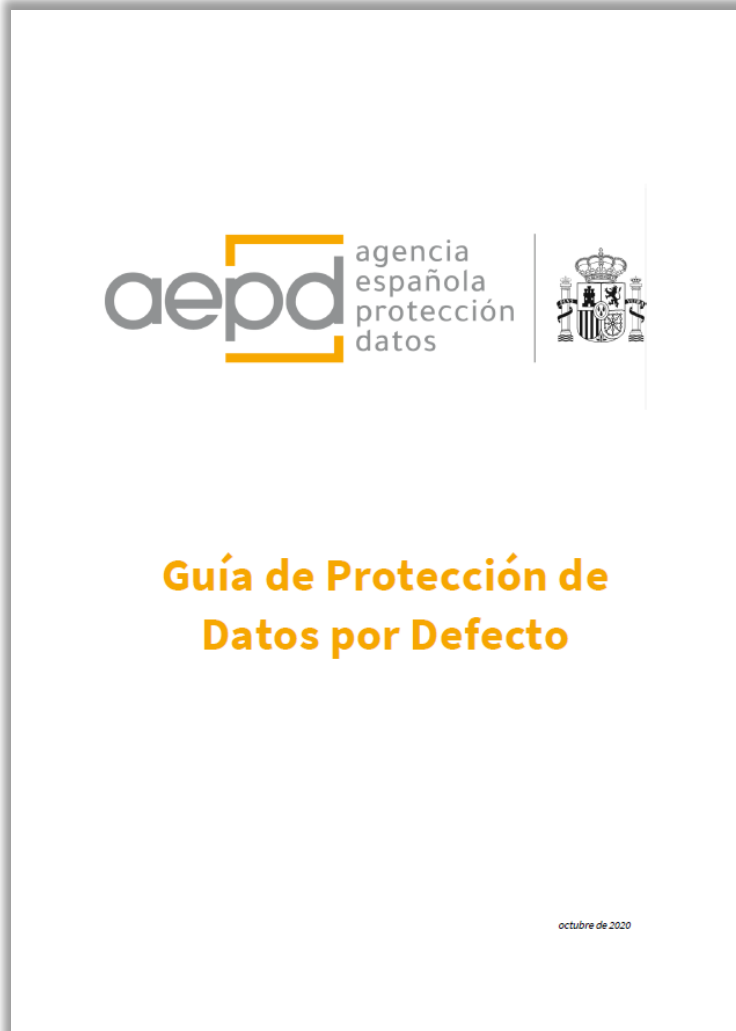
European Union Agency for Network and Information Security

www.enisa.europa.eu

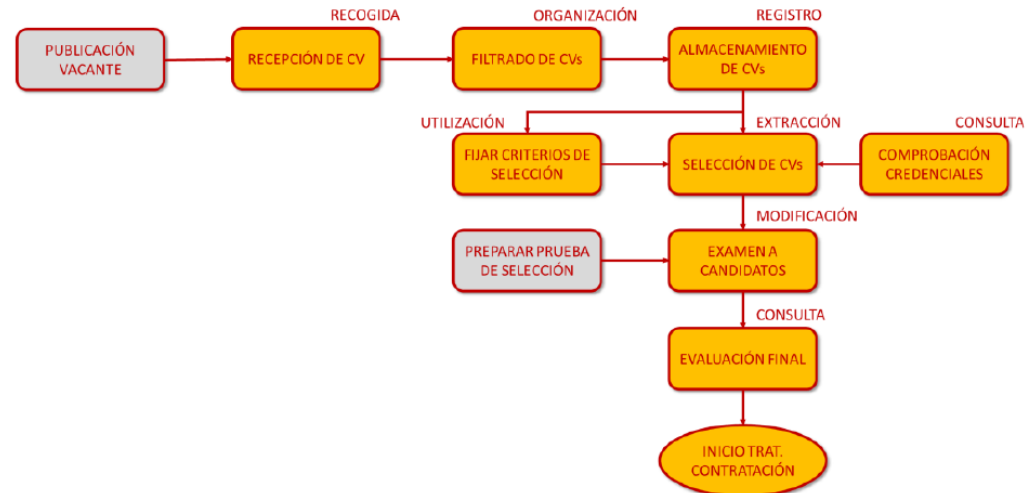
В этом исследовании представлен обзор способов и мер, которые могут быть использованы для преодоления разрыва между существующей правовой базой в сфере защиты персональных данных и имеющимися технологиями обработки информации. В документе описывается метод сопоставления юридических требований с проектными 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.

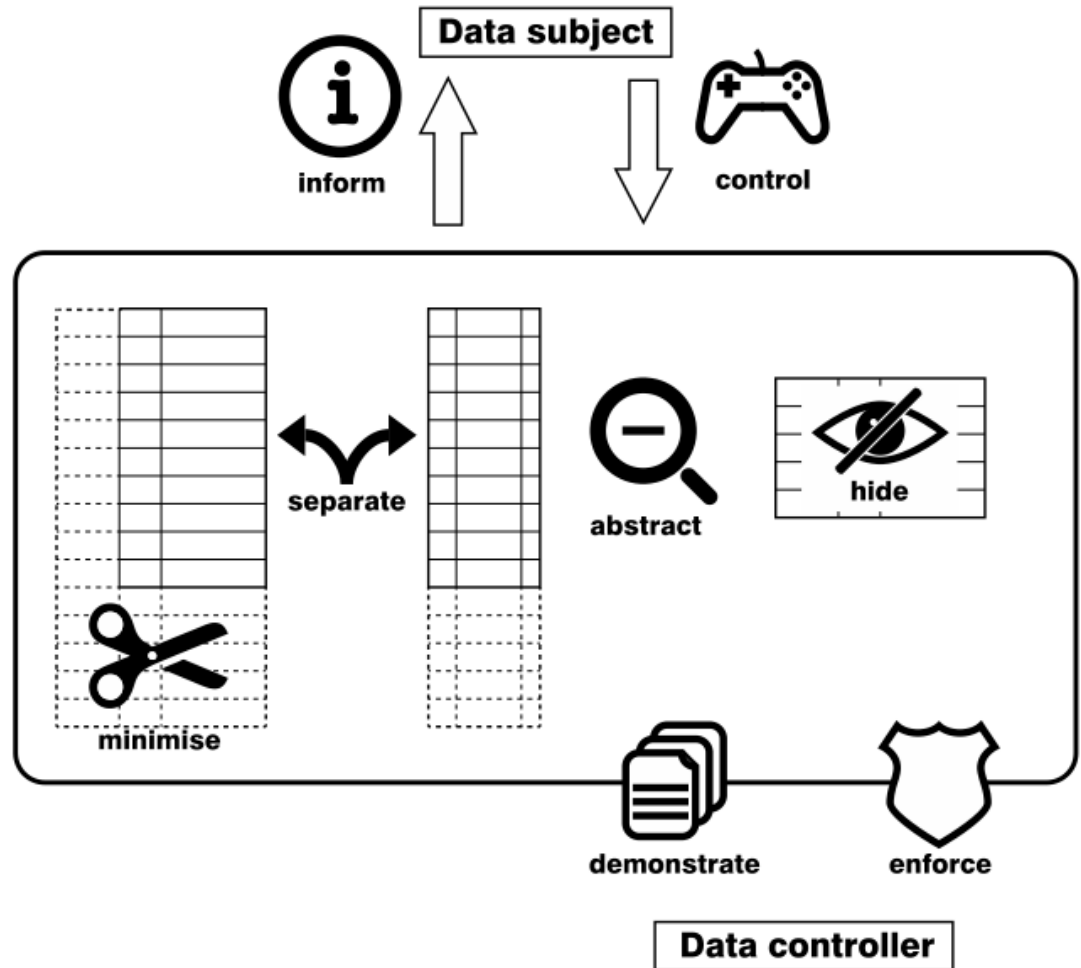


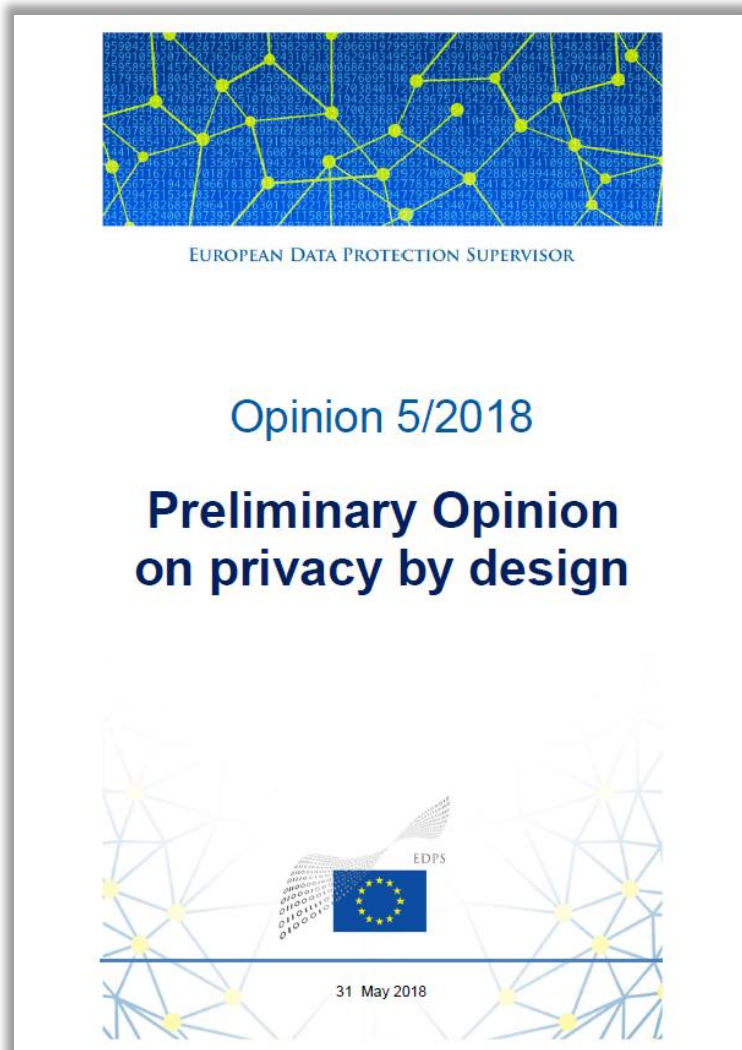




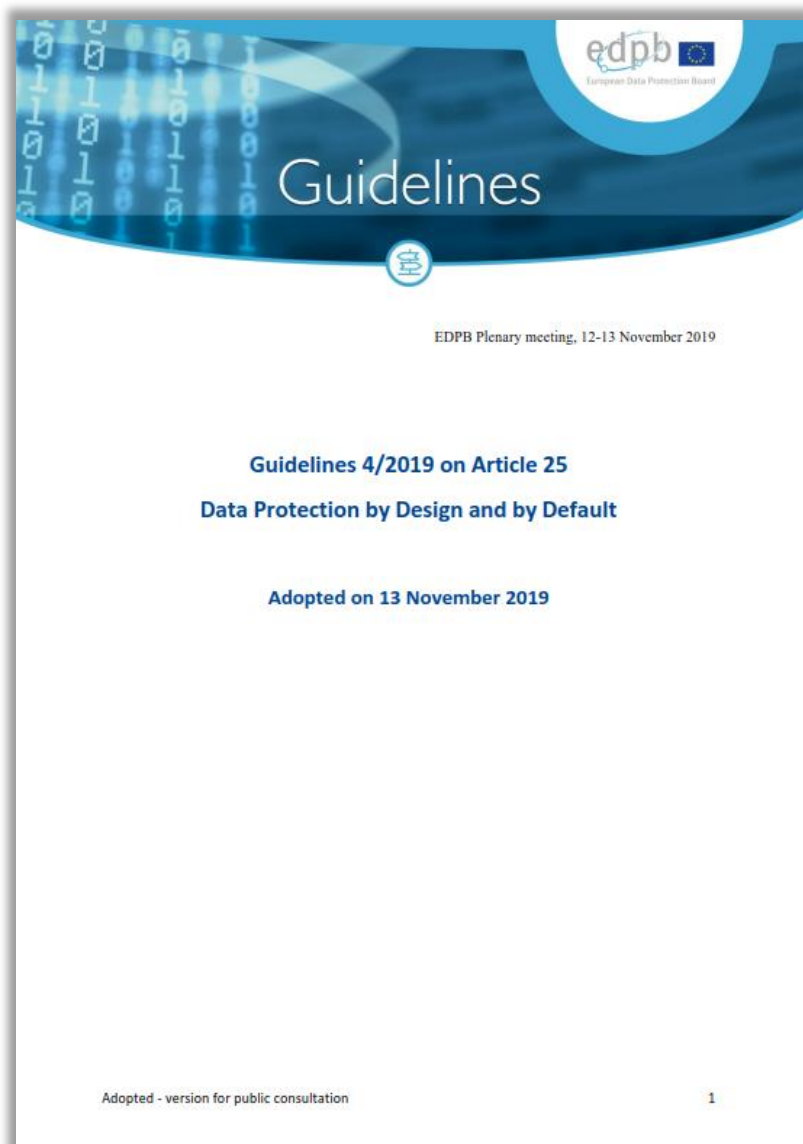
Испанский орган по защите данных (AEPD) выпустил 8 октября 2020 года руководство по практическому применению концепта Privacy by Default. В руководстве рассматриваются практические аспекты Privacy by Default, включая рекомендации по объему собираемых данных, сроку хранения и доступу к сохраняемым данным. 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».







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.



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.

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.

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.

Minimal Information Asymmetry

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

Informed Secure Passwords

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

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.

Encryption with user-managed keys

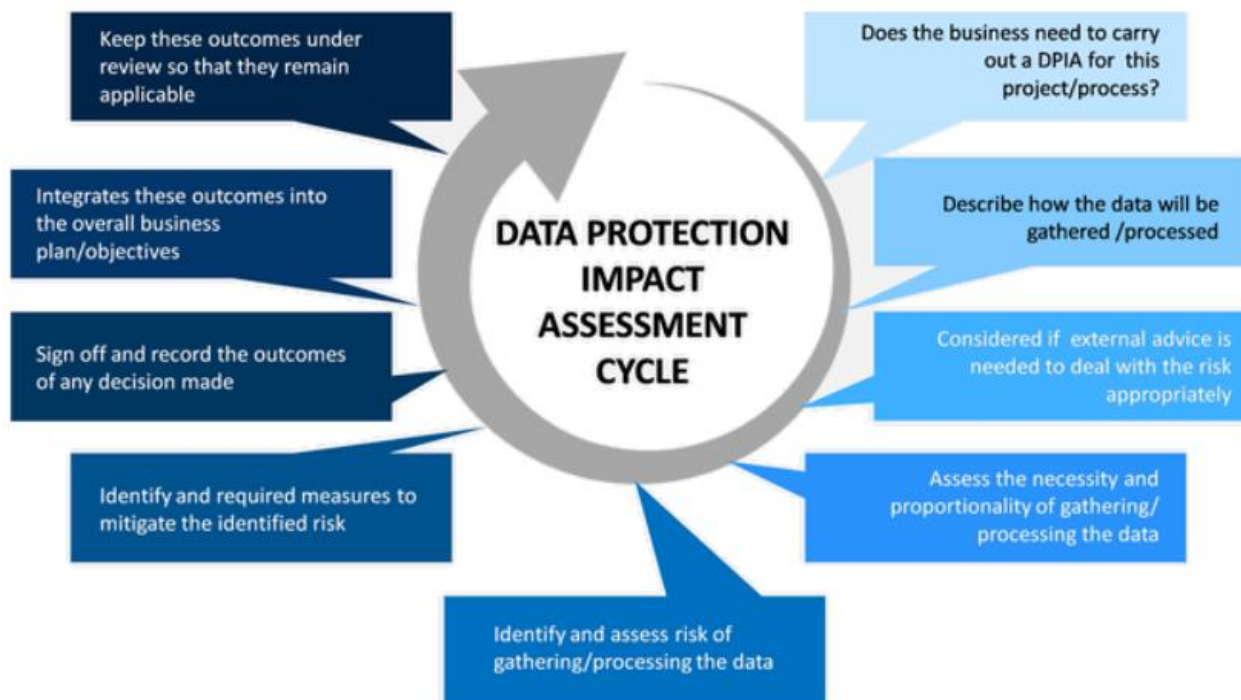
Use encryption in such a way that the service provider cannot decrypt the user's information because the user manages the keys.

Categories

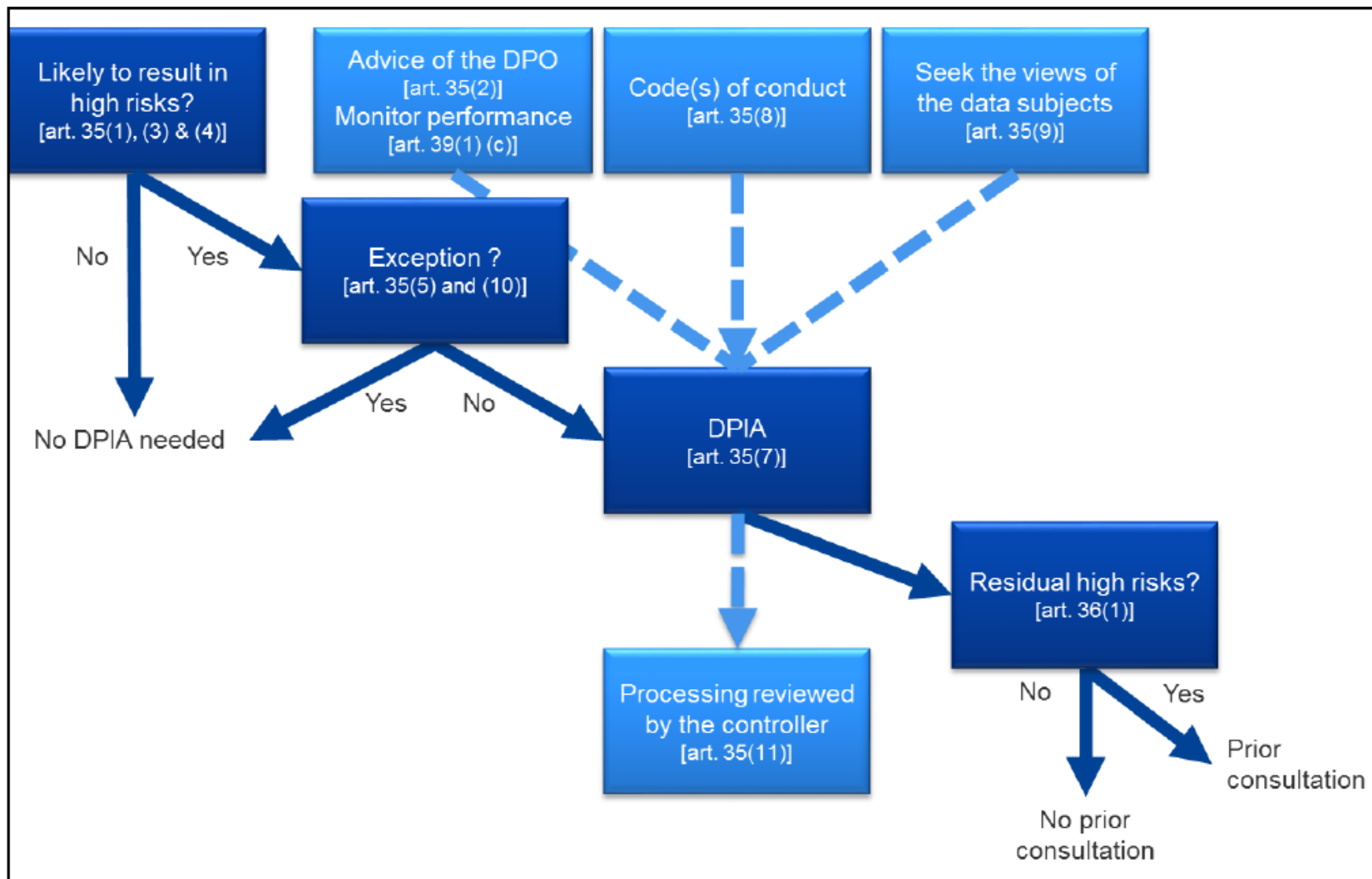
- +  CONTROL
- +  ABSTRACT
- +  SEPARATE
- +  HIDE
- +  MINIMIZE
- +  INFORM
- +  ENFORCE

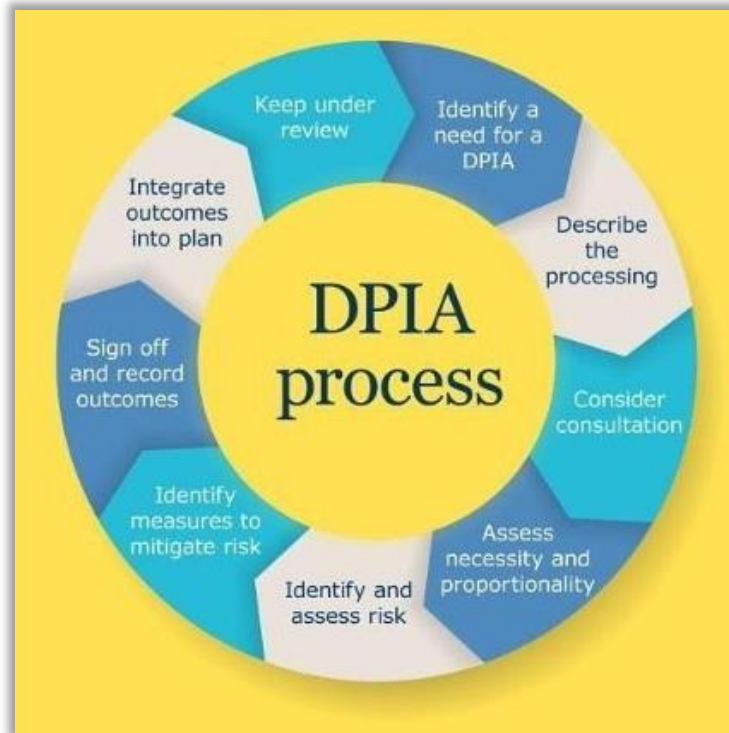
Data Protection Impact Assessment



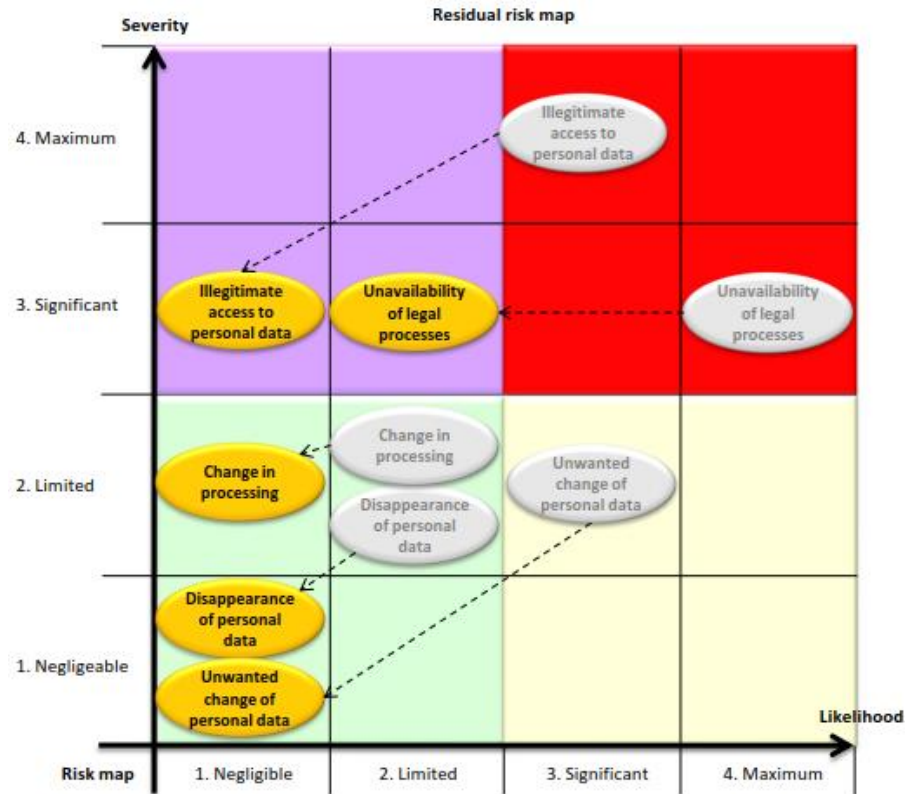
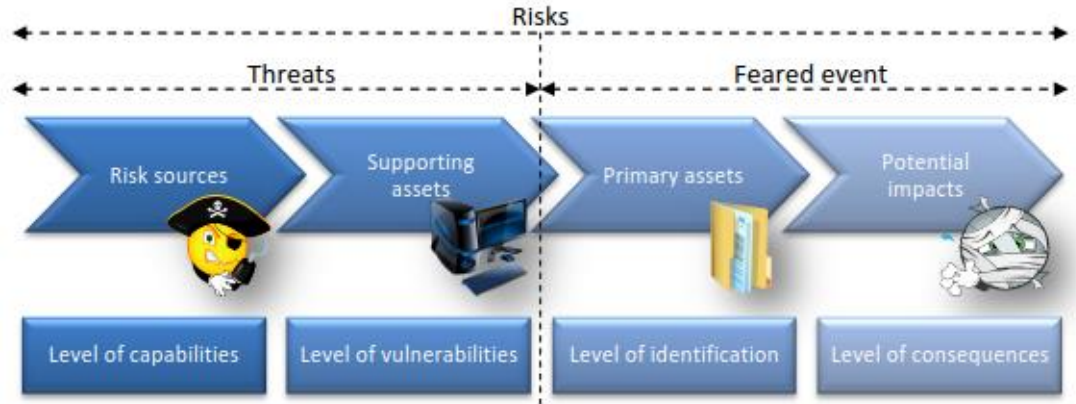
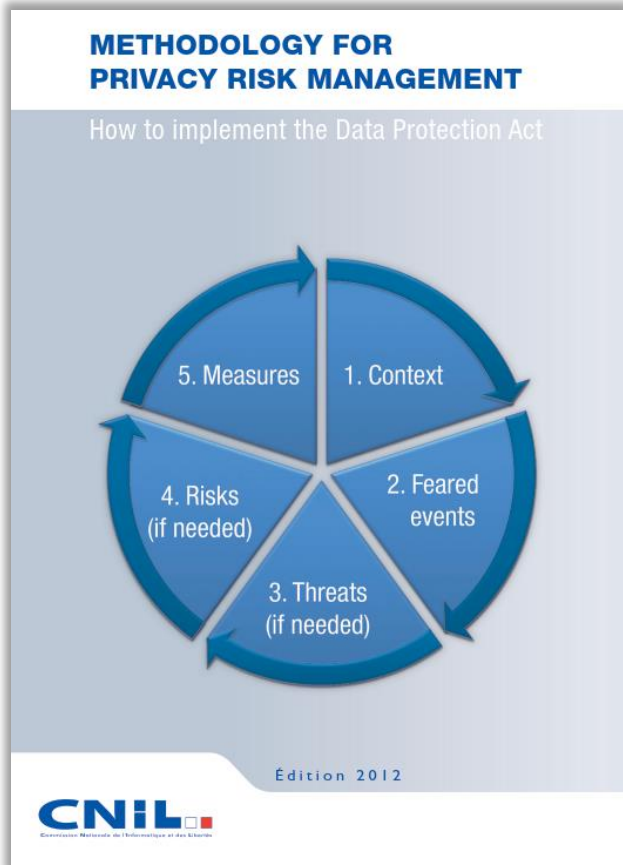


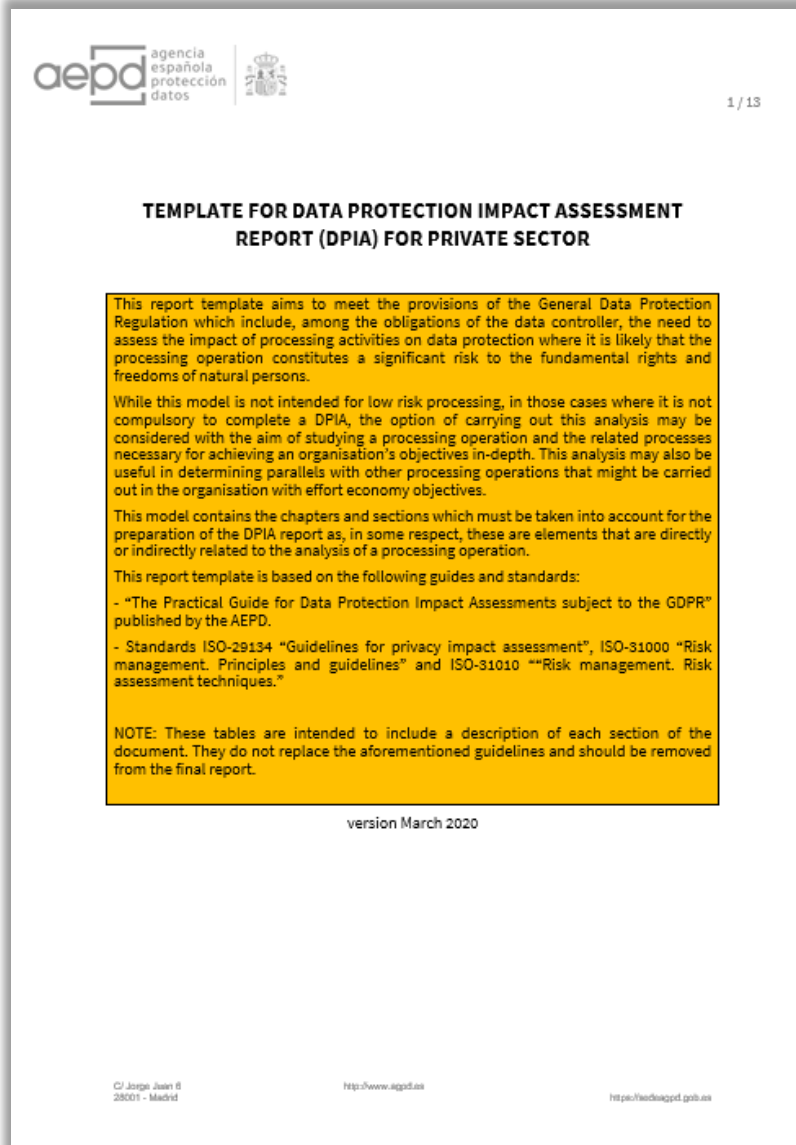
- ✓ Обязательно нужно проводить при скоринге, мониторинге, обработке больших объемов специальных категорий данных и при других аналогичных операциях с высоким риском для субъекта (передача данных за пределы ЕС, применение технических новшеств, обработка данных слабозащищённых лиц).
- ✓ контролер так 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.
- **Европейские регуляторы разъясняют, что важным аспектом для принятия решения о необходимости DPIA является качественная оценка рисков в процессах обработки персональных данных.**





Severity of impact	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
Likelihood of harm				





- 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

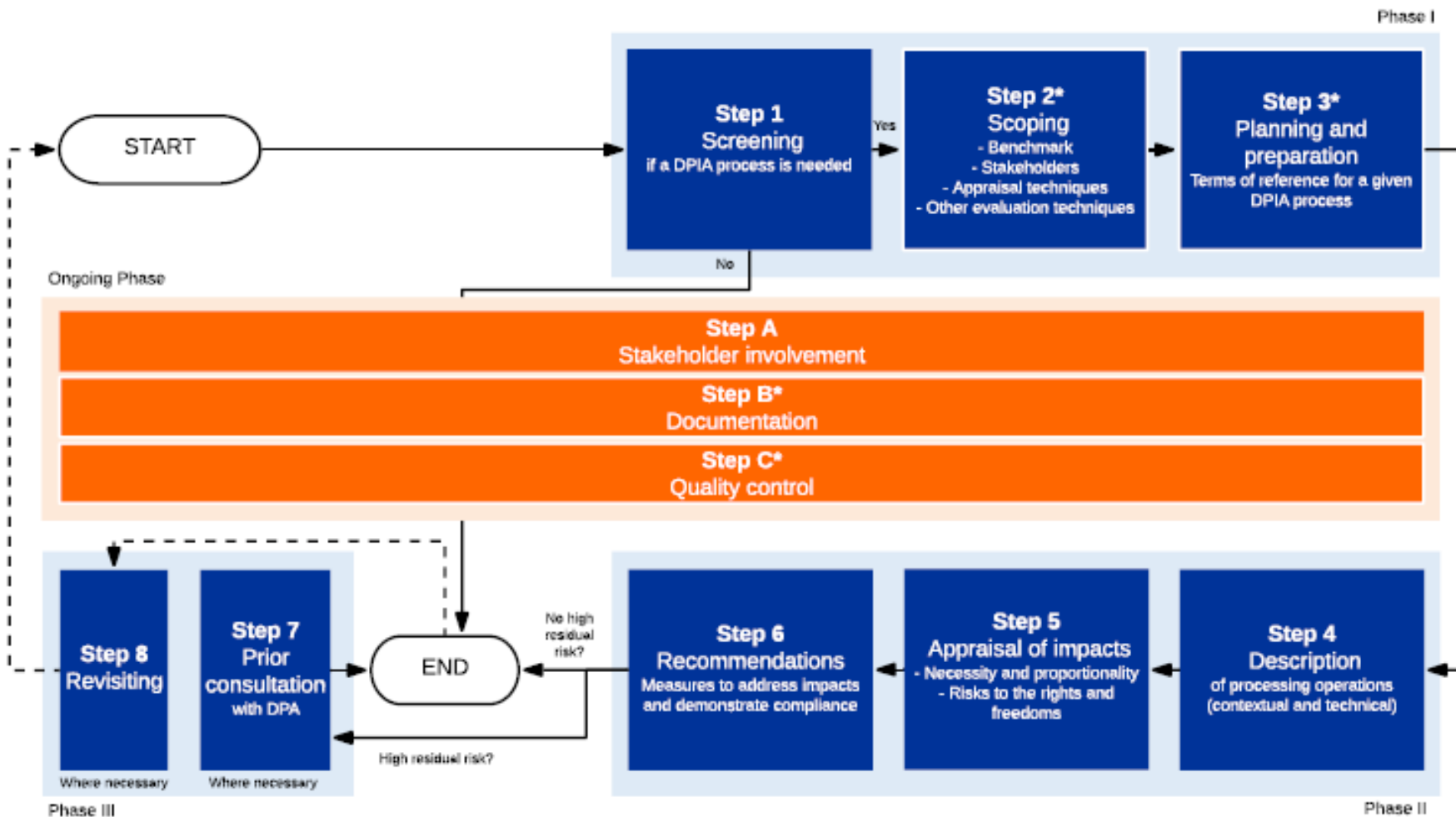
- VIII. ANALYSIS OF THE NEED FOR THE PROCESSING OPERATION

 - 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



Country	Large-scale processing	New tech	Automated decision-making	Profiling and evaluation	Location data and tracking	Combining and matching data	Employee monitoring	Public surveillance	"Invisible" processing ³	Children and vulnerable subjects	Biometric and genetic data	Data of a "highly personal nature" ⁴	Denial of service ⁵
Austria		✓	✓	✓	X	✓		✓		X	X		
Belgium	✓	✓		✓	✓						✓	✓	✓
Bulgaria		✓			✓				✓	✓	✓		
Cyprus		✓		✓		✓	✓	✓			✓		
Czech Republic	X	X					X	X		X	X	X	
Denmark		X	✓	✓	X					X	X		X
France			✓	✓	✓		✓			✓	✓	✓	✓
Germany ⁶	✓		✓	✓	✓	✓	✓	✓			X		
Hungary	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓
Ireland	✓		✓	✓	✓	✓	✓	✓	✓	✓	X		
Italy		X	✓	✓	✓	✓	✓	✓		✓	✓	✓	
Luxembourg					✓	✓	✓	✓	X		X		
Netherlands	✓	✓		✓	✓		✓	✓			✓		
Norway		X		✓	X		✓	✓			X	✓	
Poland	✓	✓	✓	✓		✓	✓	✓			✓		✓
Slovakia		X		✓		✓	✓	✓	X		X		✓
Slovenia	✓	✓	✓	✓		✓	✓	✓		✓	✓		✓
Spain	X	X	X	X	X	X	X	X		X	X	X	X
Sweden	X	X	X	X		X	✓	X		X		X	X
United Kingdom		X		✓	X	✓			X	✓	X		✓

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.

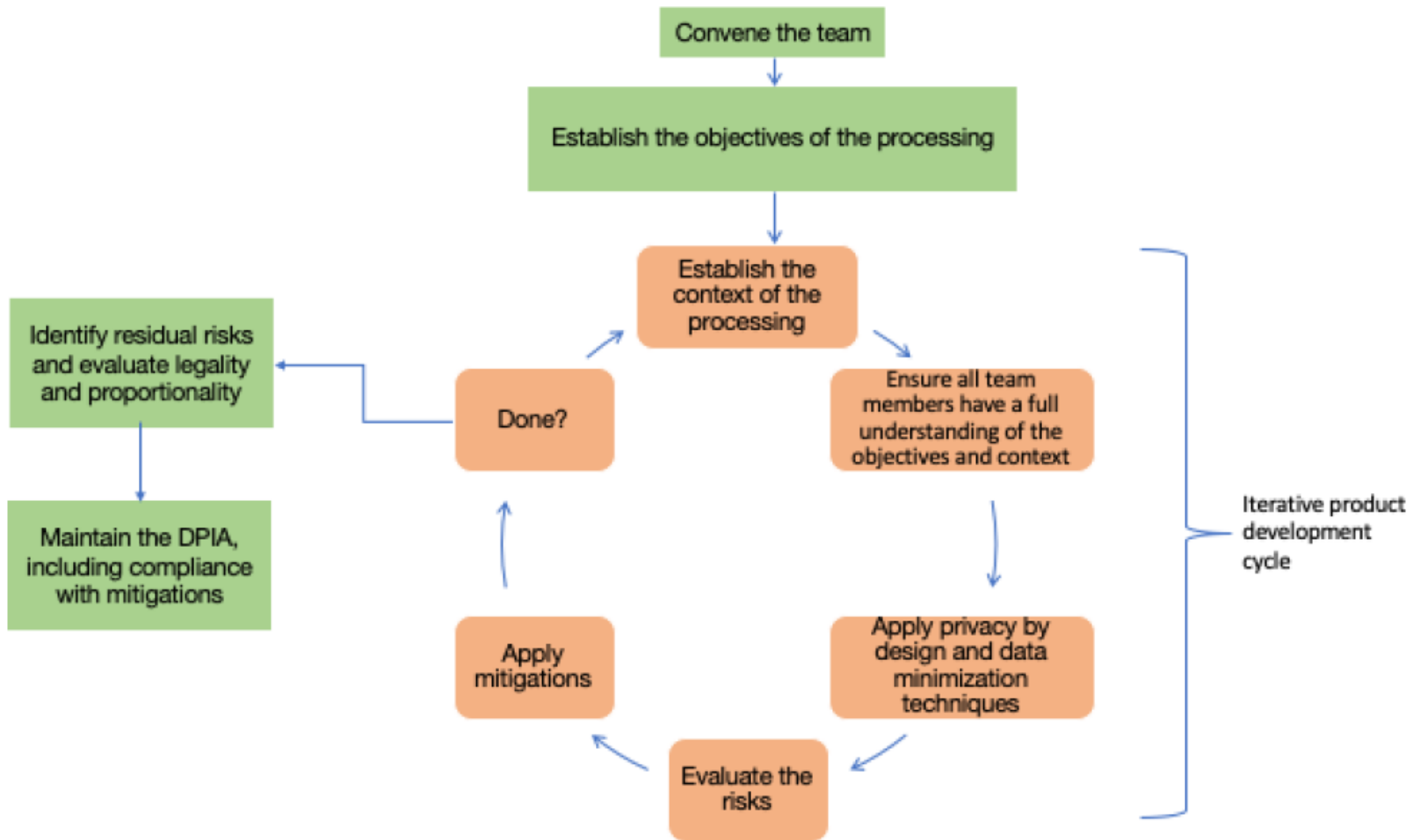
The SLM Rijk conducts negotiations with Microsoft for approximately 300.000 digital work stations of the national government. The Enterprise version of the Office software is deployed by different governmental organisations, such as ministries, the judiciary, the police and the taxing authority.

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 сотрудников в значительных масштабах, без какого-либо публичного документирования данной активности.




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).

Records of Processing Activities





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." The main navigation menu has items: Home, Your data matters, For organisations (selected), Make a complaint, Action we've taken, and About the ICO. The breadcrumb trail reads: "For organisations / Guide to Data Protection / Guide to the General Data Protection Regulation (GDPR) / Documentation /". The main heading is "How do we document our processing activities?". Below this are "Share" and "Download options" buttons. A search bar is present with the text "Search this document". A list of links on the left includes: "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?", and "How do we document our processing activities?" (highlighted). The "In detail" section contains a list of links: "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?", and "Do we need to update our record of processing activities?". The "How should we prepare?" section contains the text: "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." The "What steps should we take next?" section contains the text: "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>



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](#)



REGOLAMENTO
(UE) 2016/679





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.

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, 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 T4DATA



<p>1. What personal data or categories of personal data are collected and used for this operation?</p> <ul style="list-style-type: none"> - Given & Family Name(s) - Date of Birth - Home address - Work phone number - Private phone number - Work email address - Private email address <p>Add any further data, below if applicable:* <small>* See also below, at 2, re sensitive data</small></p>	<p><i>Tick ✓ as appropriate:</i></p>	<p>When, how and from whom are the data obtained? <small>E.g.: (data subject=DS)</small></p> <ul style="list-style-type: none"> - DWP, upon employing the person - DS, upon enrolment in research
<p>Add further rows if necessary</p>		
<p>2. Do the data you collect and record for the operation include or indirectly reveal any of the following special categories of personal data ("sensitive data")?</p> <ul style="list-style-type: none"> - Race or ethnic origin - Political opinions or affiliations - Religious or philosophical beliefs - Trade union membership - Genetic data - Biometric data - Data concerning the 	<p><i>Tick ✓ if the data is expressly collected and used for the operation;</i> <i>Tick ✓ and add ("Indirect") if the datum is indirectly revealed (explain in a note if necessary)</i></p>	<p>When and from whom are the data obtained? <small>E.g.: (data subject=DS)</small></p> <ul style="list-style-type: none"> - DWP, upon employing the person - DS, upon enrolment in research

<p>person's health</p> <ul style="list-style-type: none"> - Data concerning the person's sexual orientation or sex life - Information on criminal convictions or offences - National identifier* <small>* E.g., NI Number, Tax Number</small> - Data about debts/credit score - Data on minors 		
<p>3. If this is known or determined: How long are the (special and other) data retained? What happens then?*</p> <p><small>* 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. NB: If there are different retention periods for different data, please indicate that.</small></p>		

II.2 Disclosures of data

<p>4. To what third parties are which of the above data disclosed? And for what purposes? <small>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</small></p>	<p>Recipient third party and place and country of establishment:</p>	<p>Purpose(s) of the disclosure(s):</p>
<p>ALL THE DATA LISTED AT II.1</p>		
<p>OR: The following data: <small>(Copy the data from 1 & 2, above)</small></p> <ul style="list-style-type: none"> - - - - - - - - - - - - - - - - 		

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 ¹ Компании в процессе		
1.2.4.	Применимость законодательства ²		
1.2.5.	Основание обработки ПДн		
1.2.6.	Источники ³ 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 ⁴		
1.2.14.	Действия, совершаемые с ПДн		
1.2.15.	Распространение ⁵ ПДн		
1.2.16.	Трансграничная ⁶ 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 ⁷ 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 ⁸ третьих лиц		
1.3.2.	Страна(ы) нахождения третьих лиц		
1.3.3.	Описание функционала ⁹ третьих лиц		
1.3.4.	Основание ¹⁰ для взаимодействия с третьими лицами		
1.3.5.	Роль ¹¹ третьих лиц в процессе		
1.3.6.	Характер ¹² и способы ¹³ 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 ¹⁴ ПДн		
1.3.11.	Трансграничная передача ПДн		
1.3.12.	Длительность ¹⁵ обработки ПДн		
1.3.13.	Способ ¹⁶ обработки ПДн		
1.3.14.	Перечень ¹⁷ субобработчиков		
1.3.15.	Перечень стран для обработки ПДн		
1.3.16.	Перечень ¹⁸ 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 ¹⁹ третьих лиц		
1.3.20.	Контактные данные ²⁰ представителей третьих лиц		
1.3.21.	Контактные данные ²¹ 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.

Legitimate Interests



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?

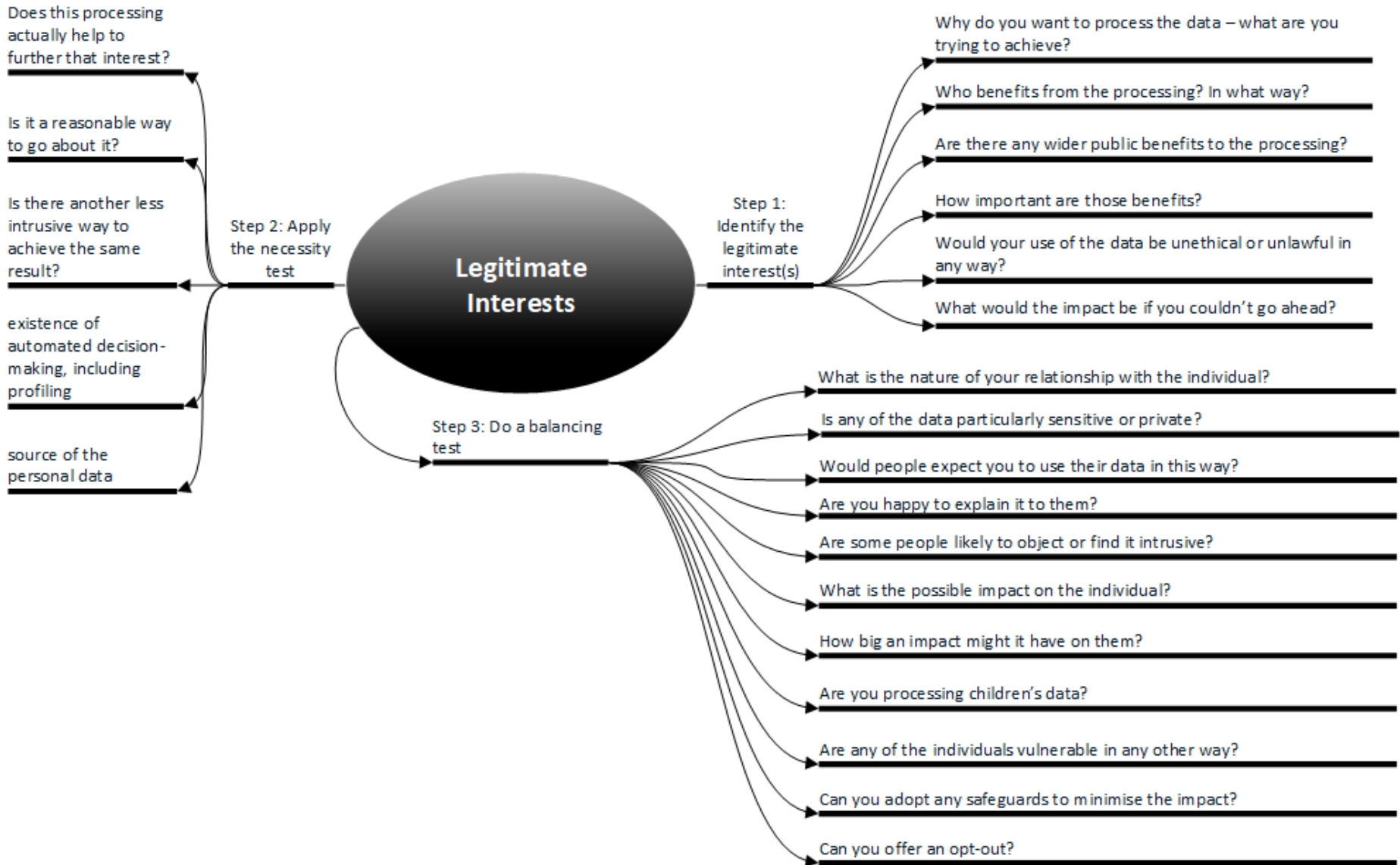
Part 3: Balancing test

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.





The cover features the Data Protection Network logo on the left and a grid of partner logos including BRISTOWS, dma, IISBA, iab, Institute of Fundraising, IPA, Balfour Beatty, driftrock, EPSILON, HARTE HANKS, and MEMBERSO. The title is centered in a large, dark font. Below the title is a photograph of a hand holding a tablet with glowing data icons floating above it. At the bottom, there is a dark blue footer with white text.

Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation

For commercial, not-for-profit organisations, and for individuals

06.04 2018 Version 2.0 Copyright of Data Protection Network. All rights reserved. 2018 ©

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:

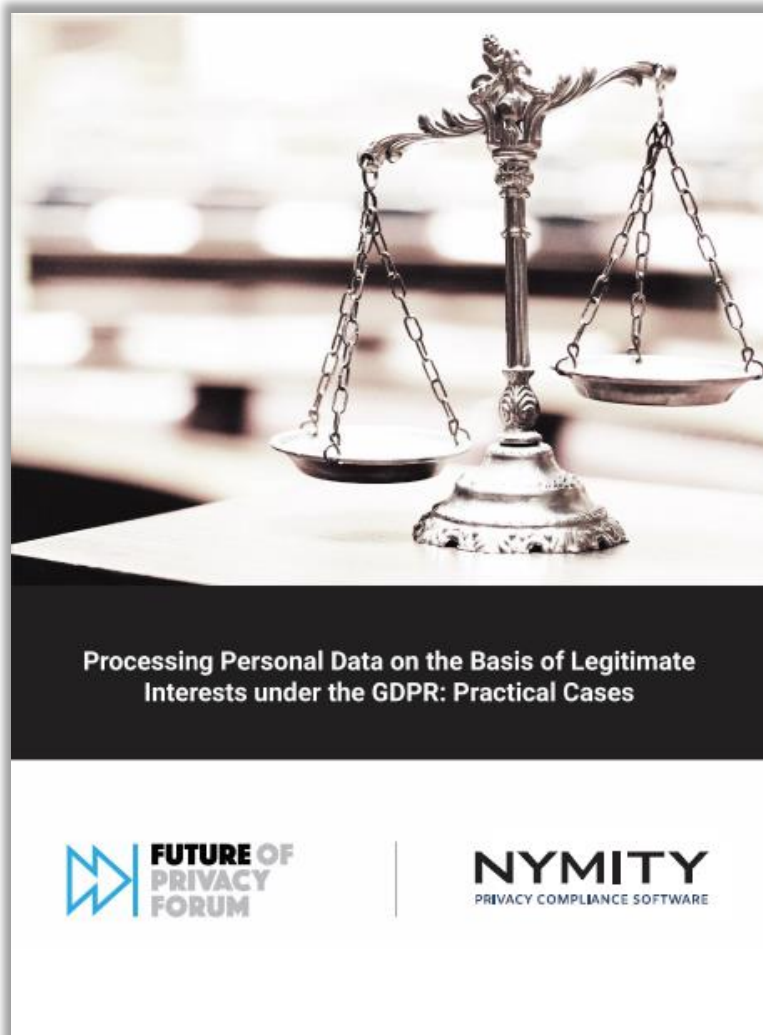
Appendix A – Legitimate Interest Process Flow for selecting Lawful Basis for processing

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



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.



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.

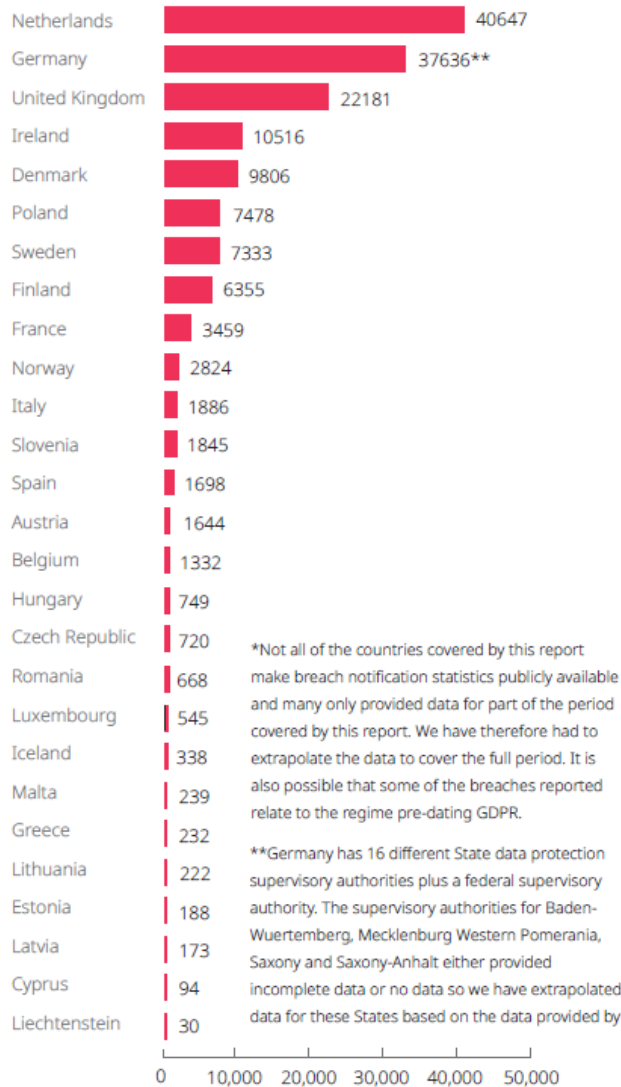
Data Breach



Статистика нарушений безопасности персональных данных в 2018-2019 годах от DLA Piper

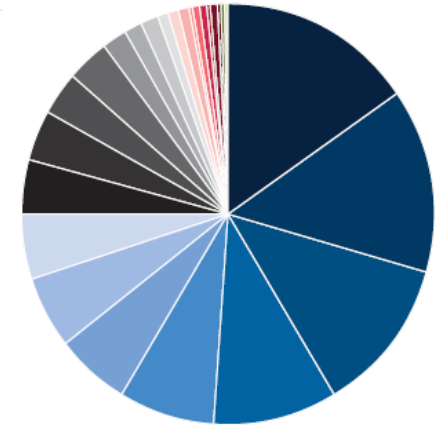


Total number of personal data breaches notified per jurisdiction for the period from 25 May 2018 to 27 January 2020 inclusive*



Per capita country ranking of breach notifications* Number of data breaches per 100,000 people for the period 28 January 2019 to 27 January 2020 inclusive Change compared to last year's ranking

Country	Per capita value	Change compared to last year's ranking
Netherlands	147.2	0
Ireland	132.52	0
Denmark	115.43	0
Iceland	91.15	+9
Finland	71.11	-1
Luxembourg	56.97	+1
Slovenia	52.55	-1
Sweden	48.14	0
Liechtenstein	39.18	-4
Norway	37.31	+2
Germany	31.12	0
Malta	31	-3
United Kingdom	17.79	-3
Poland	13.74	+1
Austria	12.1	-1
Estonia	9.74	N/A
Belgium	7.88	-1
Latvia	6.13	0
Hungary	4.87	0
Cyprus	4.8	-3
Lithuania	4.18	N/A
Czech Republic	4.03	-2
France	3.2	-2
Spain	2.08	-1
Italy	2.05	0
Romania	1.9	-2
Greece	1.5	-1



*Per capita values were calculated by dividing the number of data breaches reported by the total population of the relevant country multiplied by 100,000. This analysis is based on census data reported in the CIA World Factbook (July 2018 estimates)



Recommendations for a methodology of the assessment of severity of personal data breaches

Working Document, v1.0, December 2013




 European Union Agency for Network and Information Security www.enisa.europa.eu

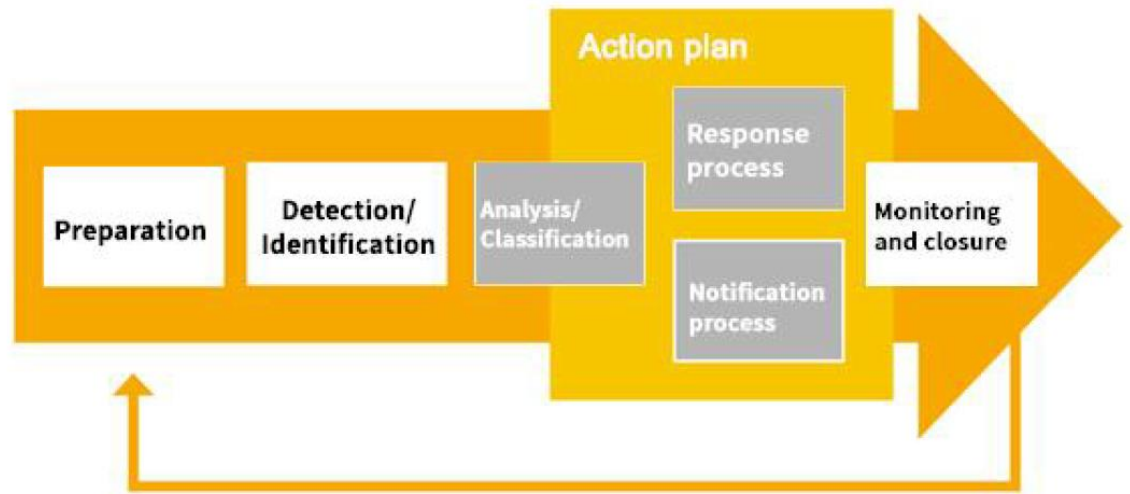
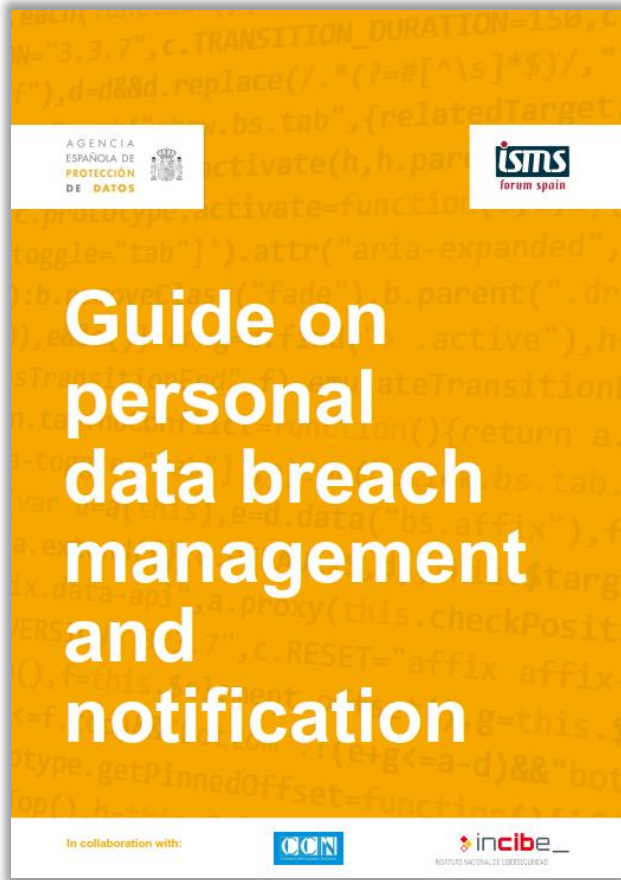
Definition of severity level

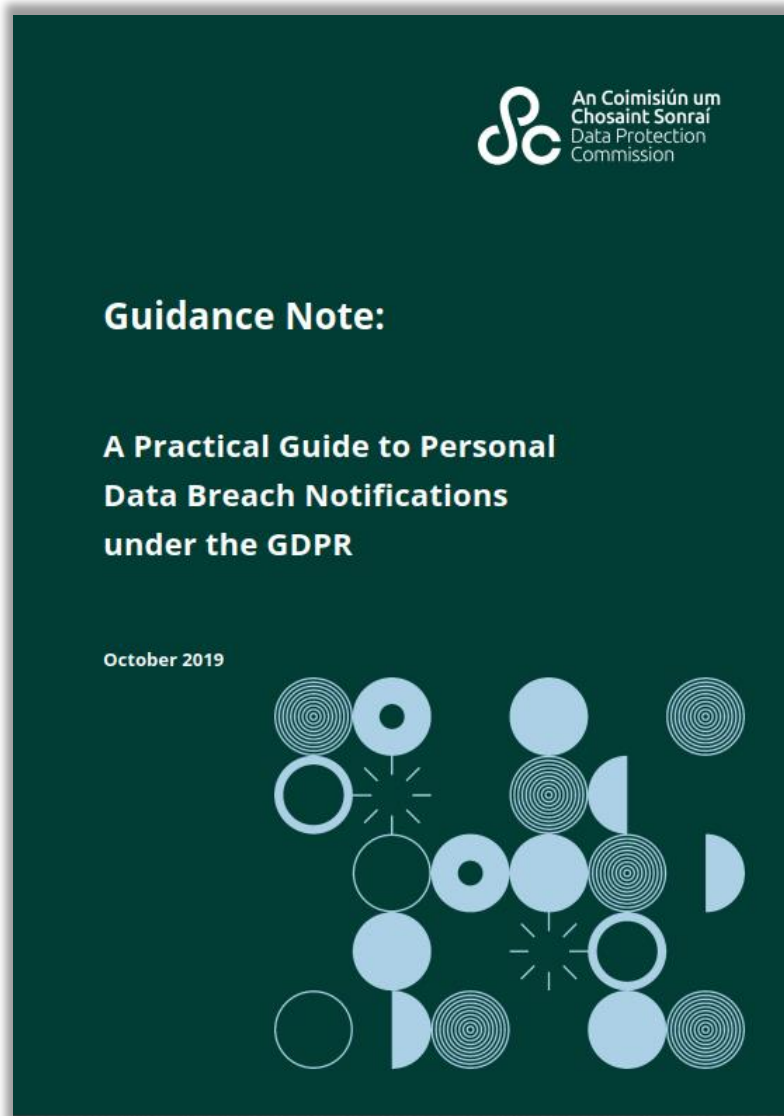
As introduced in the Section 2.2, the overall severity (SE) is calculated by the following formula:

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

The final score shows the level of severity of a certain breach, taking into account the impact to the individuals⁸.

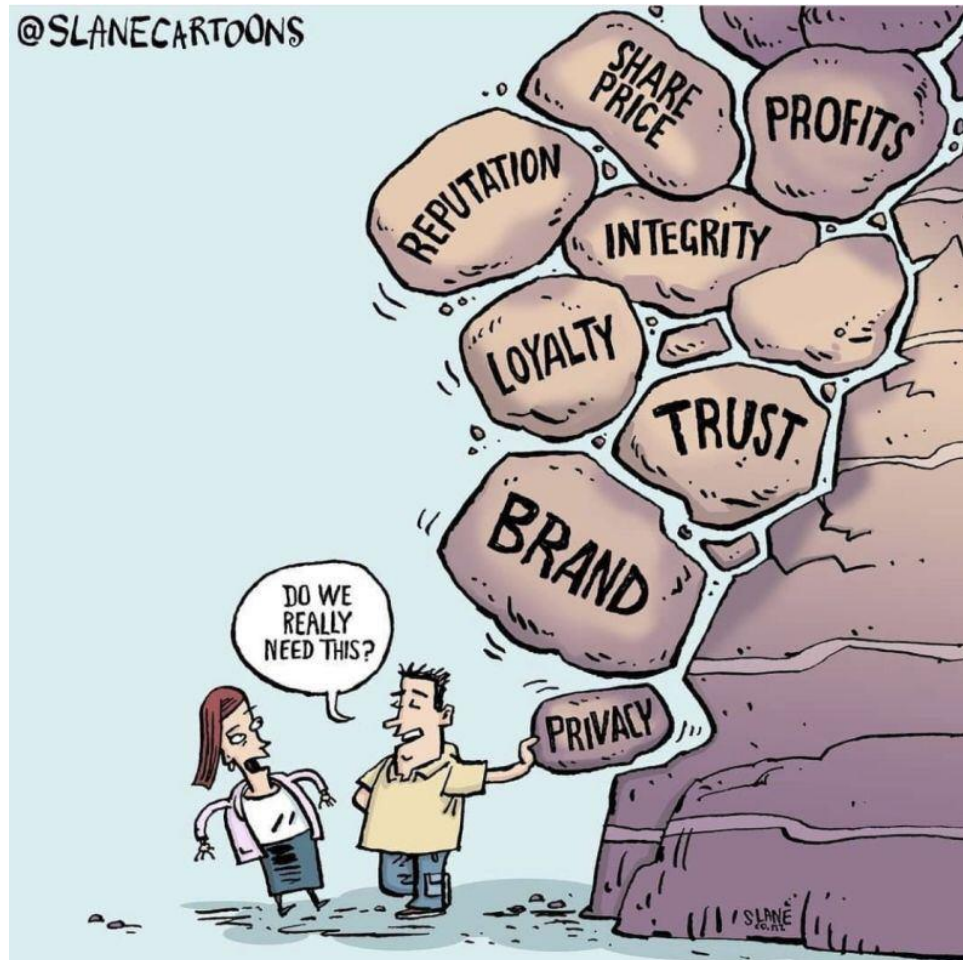
Severity of a data breach		
$SE < 2$	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
$2 \leq SE < 3$	Medium	Individuals may encounter significant inconveniences, 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.).
$3 \leq SE < 4$	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.).
$4 \leq SE$	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.).





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.

Data Protection Officer





Предварительная задача: определение сферы и контекста функционирования контролера

Организационные функции:

1. Создание и поддержание реестра процессов обработки персональных данных (RoPA)
2. Изучение и анализ процессов обработки персональных данных
3. Оценка Data Protection рисков, связанных с процессами обработки персональных данных
4. Работа с процессами, которые могут привести к «высокому риску»: проведение оценки воздействия на защиту данных (DPIA)

Контроль соблюдения функций:

5. Регулярное выполнение задач 1 - 3 (и 4)
6. Управление нарушениями безопасности обработки персональных данных (Data Breaches)
7. Проведение расследований (включая обработку внутренних жалоб) по нарушениям Data Protection

Консультативные функции:

8. Общая консультационная поддержка контролера и субъектов данных
9. Поддержка и продвижение концепта «Защита данных по умолчанию и проектируемая защита данных» (Data Protection by Default and by Design)
10. Консультирование и мониторинг соблюдения локальных актов контролера и соглашений с третьими лицами в сфере Data Protection
11. Поддержка участия контролера в кодексах надлежащего поведения и системах сертификации

Сотрудничество и консультирование с надзорными органами (DPA):

12. Сотрудничество и консультирование с DPA

Обработка запросов субъектов данных:

13. Обработка запросов субъектов данных

Информирование и повышение осведомленности:

14. Информирование и повышение осведомленности субъектов данных и иных лиц (сотрудники, партнеры, поставщики, клиенты, общественность, СМИ и т.д.)
15. 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 сотрудником 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**.



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

ARTICLE 29 DATA PROTECTION WORKING PARTY



16/EN
WP 243 rev.01

Guidelines on Data Protection Officers ('DPOs')

Adopted on 13 December 2016

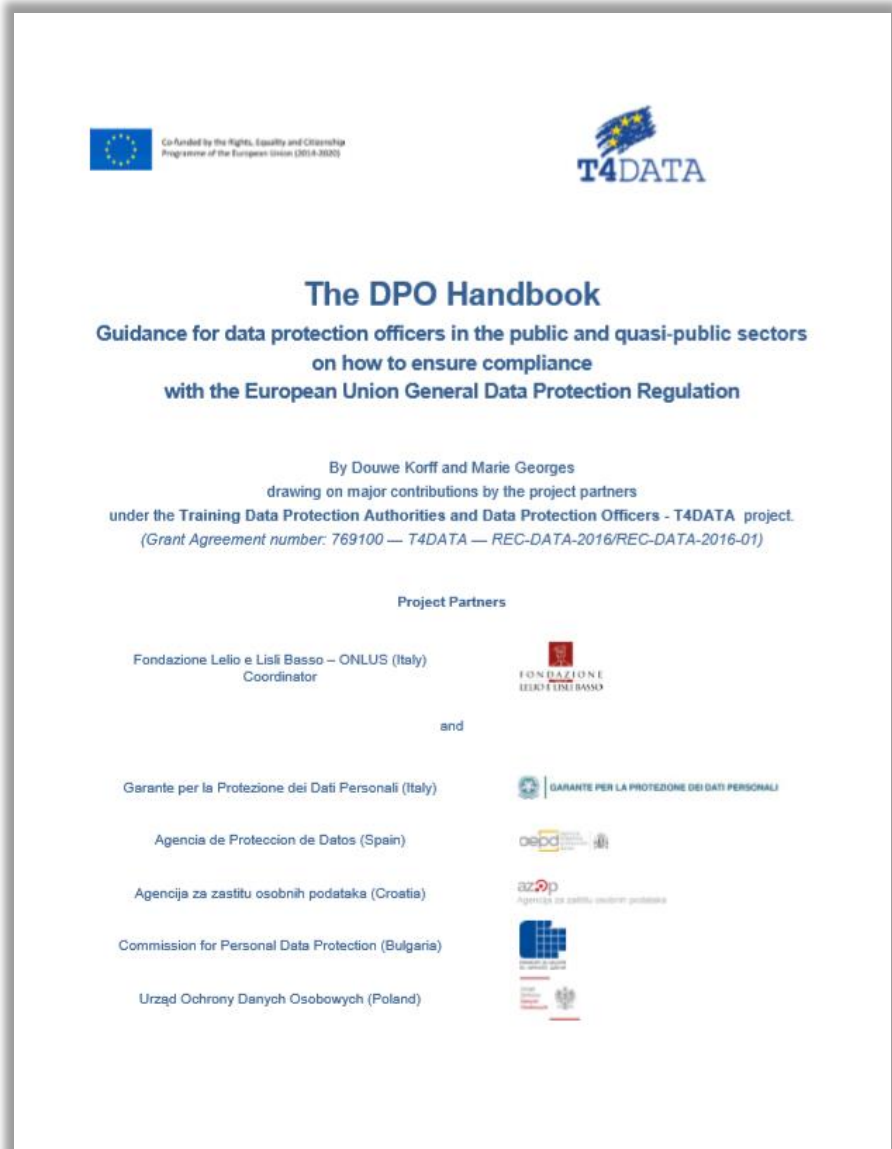
As last Revised and Adopted on 5 April 2017

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

- 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 ДРА, 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.

CNIL.*Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL |   

Certification des compétences du DPO : la CNIL adopte deux référentiels

11 octobre 2018

Afin de permettre l'identification des compétences et savoir-faire du délégué à la protection des données (DPO), la CNIL adopte deux référentiels en matière de certification de DPO.

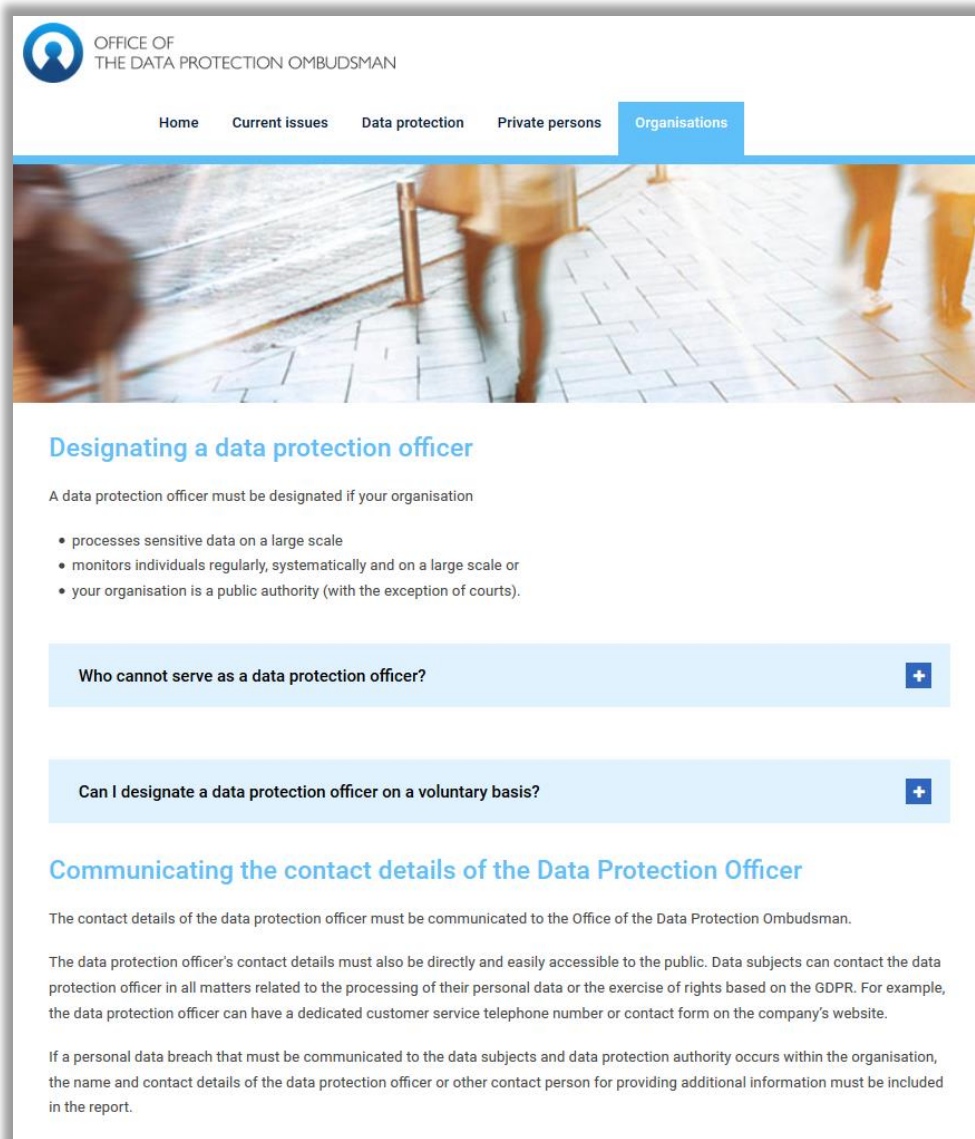
certification des compétences du DPO



Commission nationale de l'informatique et des libertés

Французский надзорный орган CNIL 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.



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.



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

DPO 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 продемонстрировала такое соответствие (подотчетность).

При выполнении своих задач DPO 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[^], sentenza del 13 settembre 2018, n°287.

DI LUIGI ROMANO 20 SETTEMBRE 2018

NEWS

Dal 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”.

TAR Friuli Venezia Giulia

Решением Административного суда региона Фриули – Венеция-Джулия в Италии (TAR Friuli Venezia Giulia) от 13.09.2018 №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.

Publicato il 13/09/2019

N. 01468/2019 REG.PROV.COLL.
N. 00182/2019 REG.RIC.



R E P U B B L I C A I T A L I A N A

IN NOME DEL POPOLO ITALIANO

Il Tribunale Amministrativo Regionale per la Puglia

Lecce - Sezione Terza

ha pronunciato la presente

SENTENZA

sul ricorso numero di registro generale 182 del 2019, integrato da motivi aggiunti, proposto da:

Rizzi Roberta, rappresentata e difesa dall'avvocato Rodolfo Barsi, con domicilio digitale come da PEC da Registri di Giustizia e domicilio eletto presso il suo studio in Lecce, viale Oronzo Quarta, 16;

contro

Comune di Taranto, in persona del legale rappresentante *pro tempore*, rappresentato e difeso dall'avvocato Angela Maria Buccoliero, con domicilio digitale come da PEC da Registri di Giustizia;

nei confronti

Istituto di Formazione Manageriale & Consulting S.r.l., in persona del legale rappresentante *pro tempore*, rappresentato e difeso dagli avvocati Giovanni Nardelli e Gerardo Carlo Federico De Letteris, con domicilio digitale come da PEC da Registri di Giustizia e domicilio eletto presso lo studio Giovanni Nardelli in Lecce, via Rubichi n. 23/A;
Neglia Teresa, non costituita in giudizio;

per quanto riguarda il ricorso introduttivo,

per l'annullamento, previa sospensione dell'efficacia:

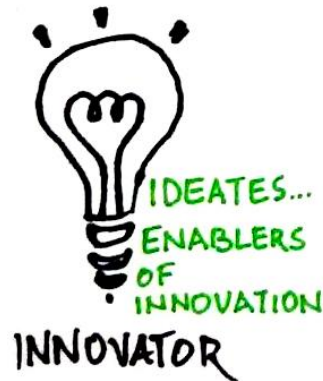
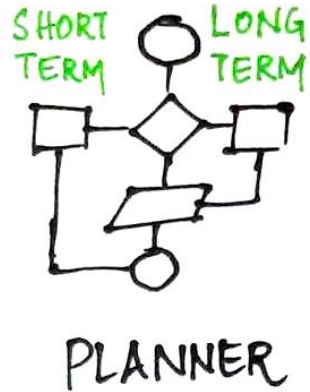
- della graduatoria finale degli ammessi al conferimento dell'incarico biennale per l'attuazione del Regolamento U.E. n. 679 del 2016 sulla protezione dei dati personali ed individuazione del Responsabile per la Protezione dei Dati (R.P.D.), graduatoria formulata all'esito della procedura di gara informale svolta, ai sensi dell'art. 36, comma 2, lett. a), del D. Lgs. n. 50/2016, dal Comune di Taranto e pubblicata sul sito del predetto Comune, in parte *qua*,
- della determina n. 400/2018 del 21 dicembre 2018, con cui il Dirigente del Settore Sviluppo Economico e Produttivo del Comune di Taranto ha approvato l'attività della Commissione giudicatrice ed ha disposto l'aggiudicazione della predetta gara nei confronti dell'Istituto di Formazione Manageriale & Consulting S.r.l.;

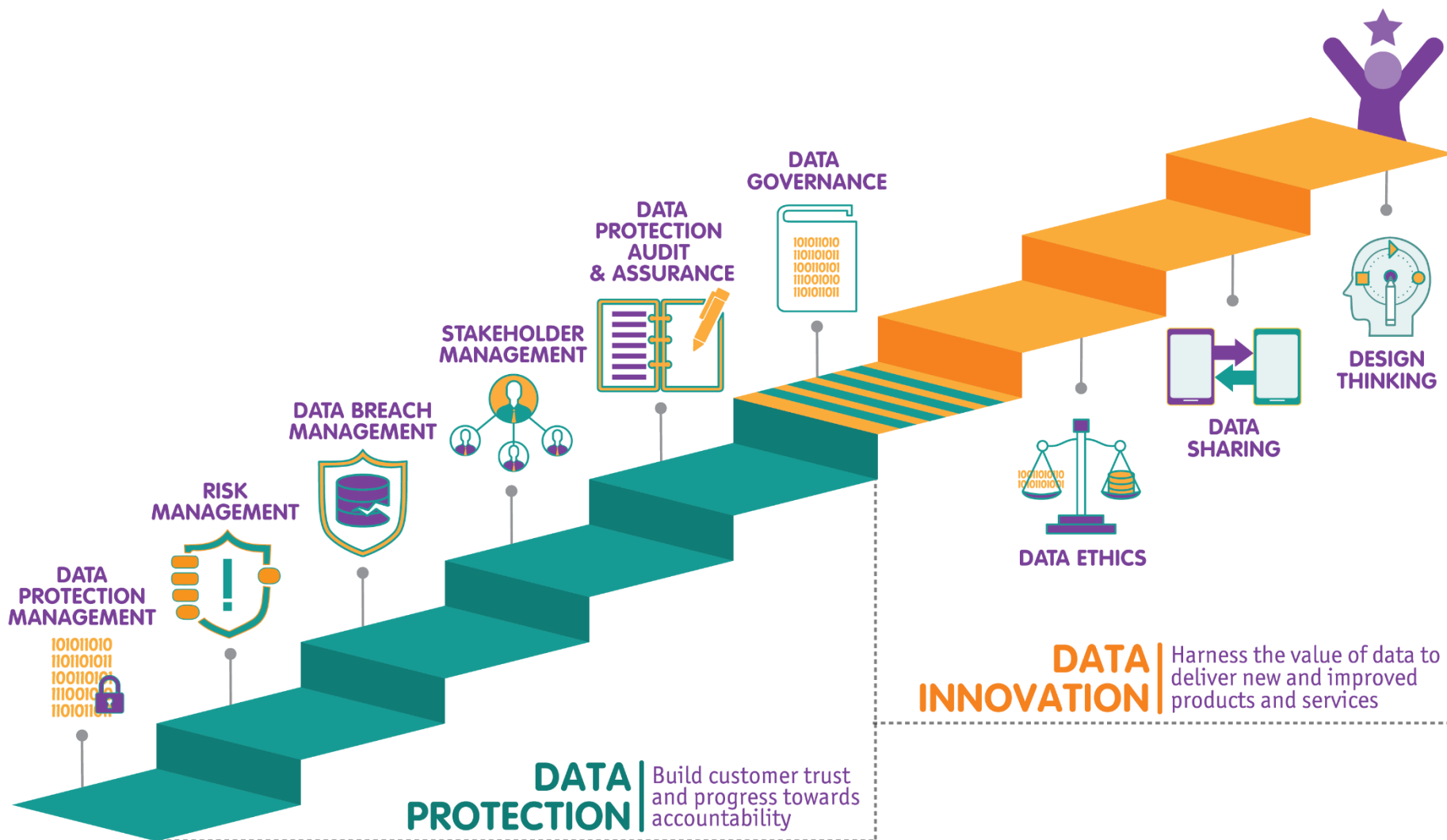
TAR Friuli Venezia Giulia

Решением Административного суда региона Апулия – Лечче в Италии (TAR Puglia – Lecce) от 13.09.2019 №287 указано, что при аутсорсинге функции DPO посредством заключения контролером договора со сторонней компанией внешний DPO должен быть сотрудником нанятой компании. Другими словами, невозможно нанять компанию в качестве внешнего DPO и позволить этой компании также нанять субпорядчика 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)





THE IRISH TIMES Sun, Dec 9, 2018

NEWS SPORT **BUSINESS** OPINION LIFE & STYLE CULTURE

The Economy | Your Money | Companies | Technology | Work | Commercial Property | Co

Data watchdog investigating potential GDPR breaches in Government

Department of Social Protection allegedly interfered with role of its data protection officer

© Thu, Dec 6, 2018, 06:20 | Updated: Thu, Dec 6, 2018, 07:11

Elaine Edwards



Over three million photographs are held in the department's facial matching database for the public services card

⋮ The Data Protection Commission has said it is investigating “potential breaches” of the General Data Protection Regulation by a Government department, following a complaint that it allegedly interfered with the role of its data protection officer, an offence under the EU legislation.

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.

<https://www.irishtimes.com/business/data-watchdog-investigating-potential-gdpr-breaches-in-government-1.3721640>

<https://www.thetimes.co.uk/article/department-of-employment-and-social-protection-may-face-gdpr-fine-of-up-to-1m-0hcrrlh3>

131 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 департаментов 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).

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
 ✉ 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

- Procedimiento Nº: PS/00417/2019

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: A.A.A., y B.B.B. (en adelante, los reclamantes) con fecha 21 de mayo y 4 de noviembre de 2019 respectivamente interpusieron reclamación ante la Agencia Española de Protección de Datos.

Sus reclamaciones se dirigen contra **GLOVOAPP23, S.L.** con NIF **B66362906** (en adelante, el reclamado).

Los motivos en que basan su reclamación son que no tienen nombrado un Delegado de Protección de Datos (en adelante DPD) al que dirigir las reclamaciones.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 2 de julio de 2019, la primera reclamación fue trasladada a la reclamada la reclamación presentada para su análisis y comunicación al reclamante de la decisión adoptada al respecto.

La reclamada contesta al traslado de la reclamación afirmando que no se encuentran ni entre los supuestos del art. 37 RGPD ni el del 34 LOPGDD, con lo que no tienen obligación de designar un DPD.

TERCERO: Con fecha 13 de enero de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del artículo 37 del RGPD, tipificada en el artículo 83.4 del RGPD.

CUARTO: Notificado el 22 de enero de 2020 el citado acuerdo de inicio, el reclamado presentó el 31 de enero de 2020 escrito de alegaciones en el que, en síntesis, manifestaba que su actividad de tratamiento de datos personales se encuentra exenta de las obligaciones establecidas en los artículos 37 RGPD y 34 LOPGDD, y, por tanto, exenta de la obligación de designar un Delegado de Protección de Datos.

Sin embargo, alega que en ningún momento ha negado la existencia de un órgano que se dedicara, en el contexto de la organización, al desempeño de las funciones que son propias de un Delegado de Protección de Datos, ya que el 8 de junio de 2018, constituyó el Comité de Protección de Datos, con el fin de cubrir los ámbitos técnicos de la empresa y en la misma fecha, se designó también un Subcomité de Protección de Datos, a fin de dar cumplimiento a la autorización del Consejo de Administración de constituir dicho comité.

Concluye afirmando que el Comité de Protección de Datos, lleva a cabo las funciones propias de un Delegado de Protección de Datos descritas en el artículo 39 del RGPD.

Кто: Agencia Española de Protección de Datos (Испания)

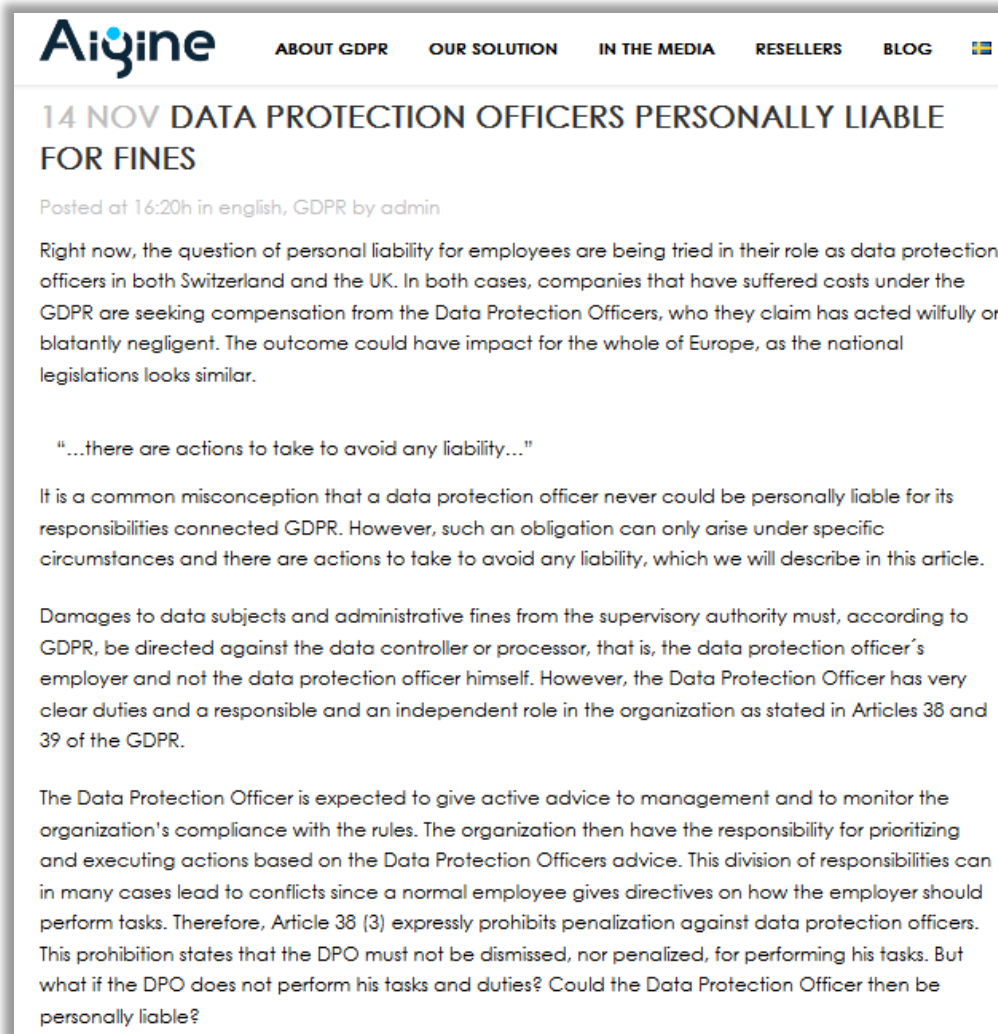
Кого: Glovoapp23 SL

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.



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.



PRIVACY & INFORMATION SECURITY LAW BLOG
Global Privacy and Cybersecurity Law Updates and Analysis

[Home](#) » [South Korean Court Imposes Personal Liability On Privacy Officer For Data Breach](#)

South Korean Court Imposes Personal Liability on Privacy Officer for Data Breach

Posted on January 9, 2020
POSTED IN [ENFORCEMENT](#), [INTERNATIONAL](#)

According to *MLex*, on January 6, 2020, the Seoul Eastern District Court found Kim Jin-Hwan, a privacy officer of the South Korean travel agency Hana Tour Service Inc., guilty of negligence in failing to prevent a 2017 data breach that affected over 465,000 customers of the agency and 29,000 Hana Tour employees.

The privacy officer was accused of violating South Korea's Personal Information Protection Act and the Network Act, which require the person responsible for the management of personal data to take necessary "technological and managerial measures" to prevent data breaches and to notify the Korea Communication Commission of any data breach incidents within 24 hours.

The Court imposed a penalty of 10 million South Korean Won (₩) against the privacy officer, which is roughly equivalent to \$8,500. This is in addition to separate fines of ₩327,250,000 (around \$280,000) imposed against the company by the Ministry of Interior and Safety.

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 сотрудников Hana Tour.

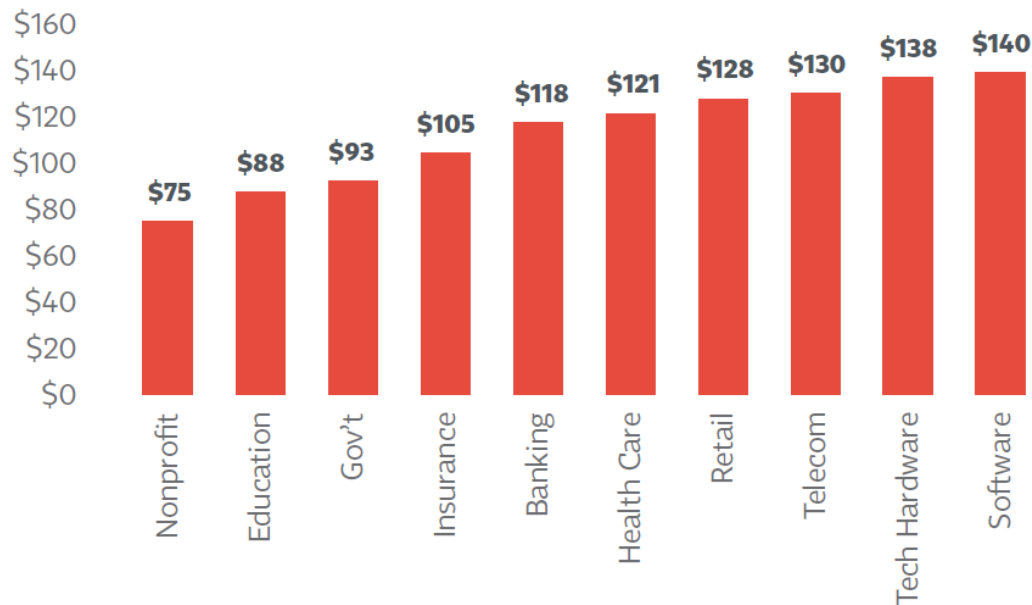
DPO был обвинен в нарушении Закона о защите персональной информации и Закона о сетях, в соответствии с которыми DPO должен принимать необходимые «технологические и управленческие меры», чтобы предотвратить утечку данных, а также обязан уведомлять Комиссию по связи Кореи о любых случаях нарушения безопасности 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.

Богаче всего Privacy Professionals живется в США (средний годовой доход в \$150,000), а в Великобритании (\$101,000), ЕС (\$98,000) и Канаде (\$72,000) все не так радужно. Средняя же годовая зарплата по указанным регионам выросла со \$111,000 в 2015г. до \$123,000 в 2019г. – почти на 11% за 4 года. Интересные факты:

1. все увеличивающееся многообразие в наименовании прайваси-функций в организациях, что говорит о постепенном росте зрелости этого направления с точки зрения специализации функционала;
2. большая диспропорция по доходам внутри отрасли инхаузов, где Chief Privacy Officer увеличили свой средний доход со \$139,000 в 2015г. до \$200,000 в 2019г. – на 44% за 4 года.

Privacy Professionals' Median Salary (In U.S. \$000)



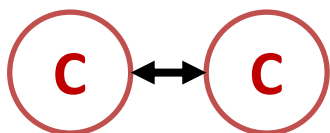
- Chief privacy officer: \$200,000
- Lead privacy counsel: \$183,000
- Director of privacy: \$147,000
- Deputy chief privacy officer: \$141,000
- Privacy engineer: \$136,000
- Data privacy manager: \$134,000
- Privacy counsel: \$130,000
- Privacy officer: \$121,000
- Privacy manager: \$105,000
- Data protection officer: \$100,000
- Privacy analyst: \$76,000

Соглашения об обработке и защите персональных данных

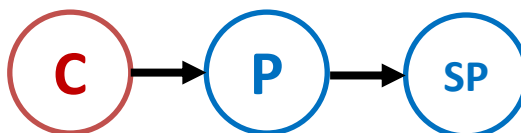


Соглашение – универсальный инструмент регулирования обработки и защиты персональных данных в GDPR

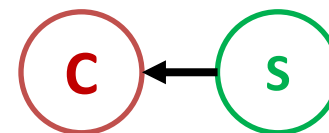
Существует большой потенциал такого универсального юридического инструмента как соглашение для урегулирования отношений об обработке и защите персональных данных между сторонами. Наиболее распространёнными и известными видами соглашений являются **DTA** и **DPA**. Стороной соглашения с контролером может 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)

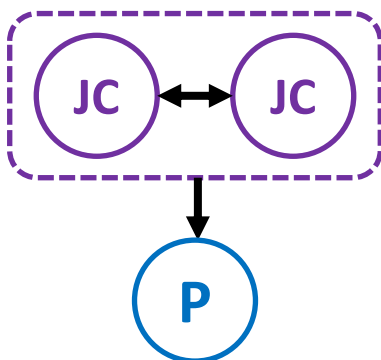


Data Processing Agreement
(Controller-to-Processor/Subprocessor)

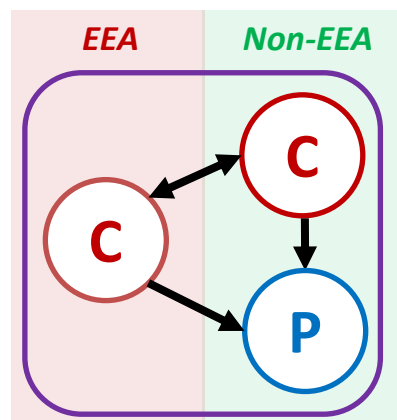


Subject's Privacy Addendum
(Controller-to-Subject)

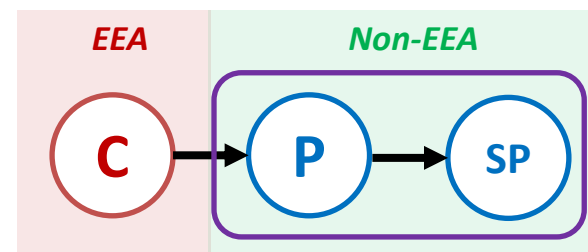
При этом GDPR фактически устанавливает режим большего разнообразия видов договорных отношений между участниками обработки персональных данных. Примером этого являются соглашения, направленные на структурирование сложных и часто трансграничных процессинговых активностей – **DMA** и механизм **BCR-C / BCR-P**.



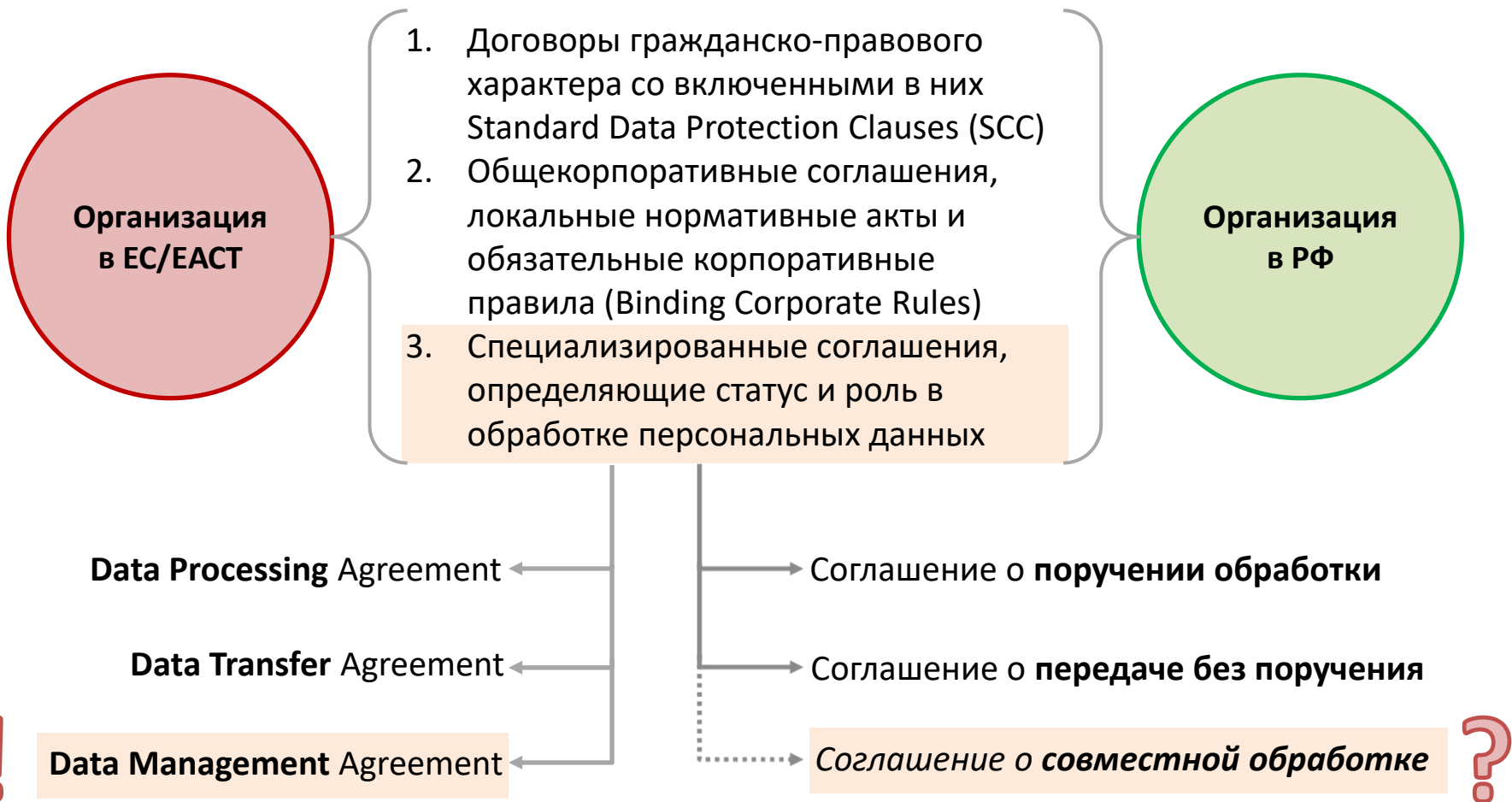
Data Management Agreement
(Joint Controllers)



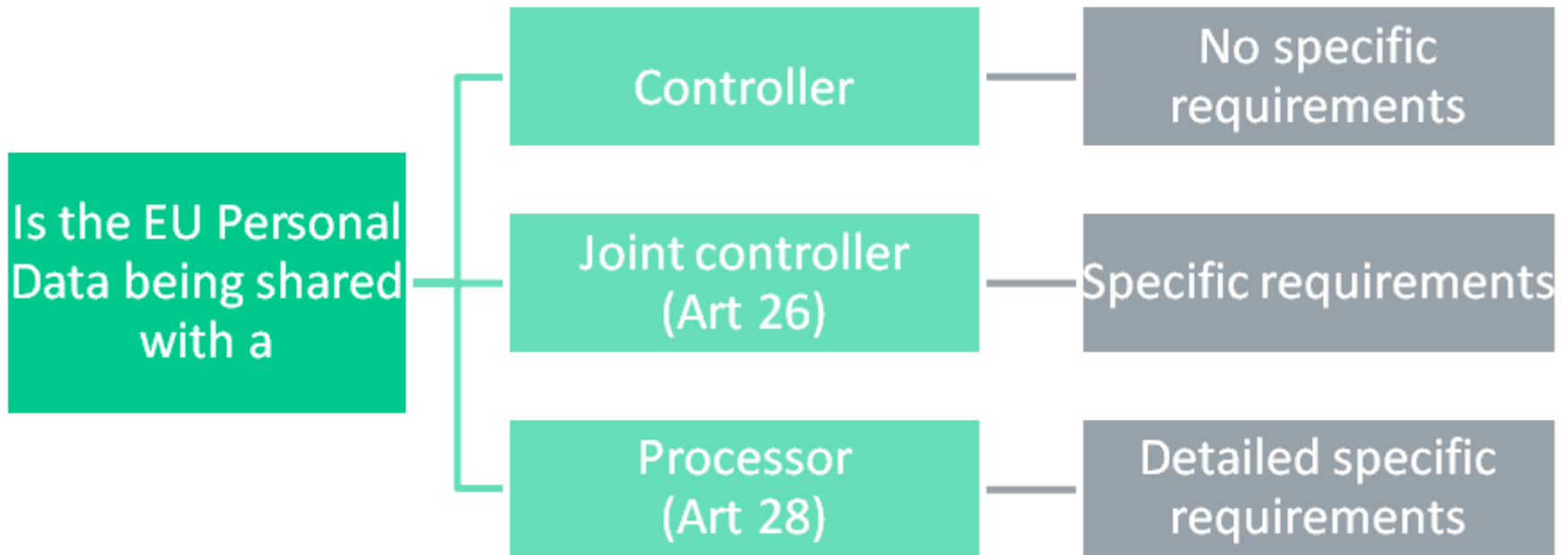
Binding Corporate Rules – C
(Controller)

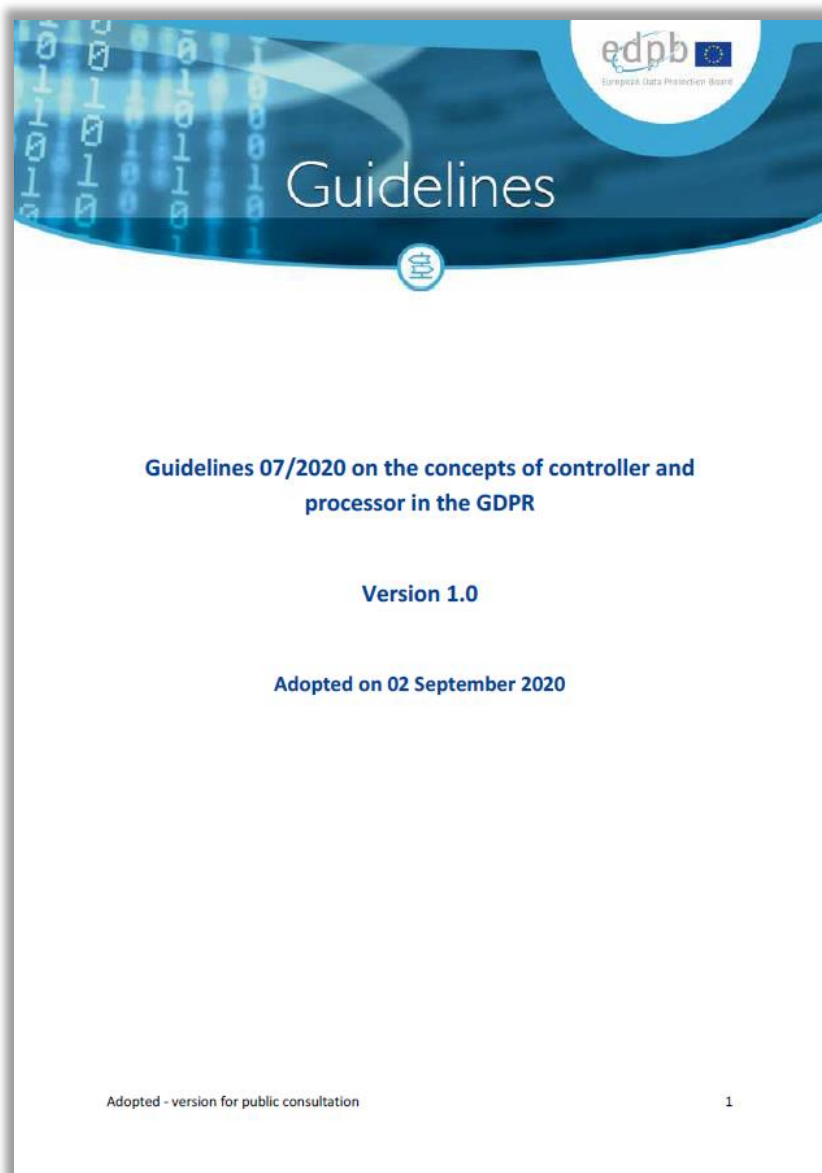


Binding Corporate Rules – P
(Processor/Subprocessor)

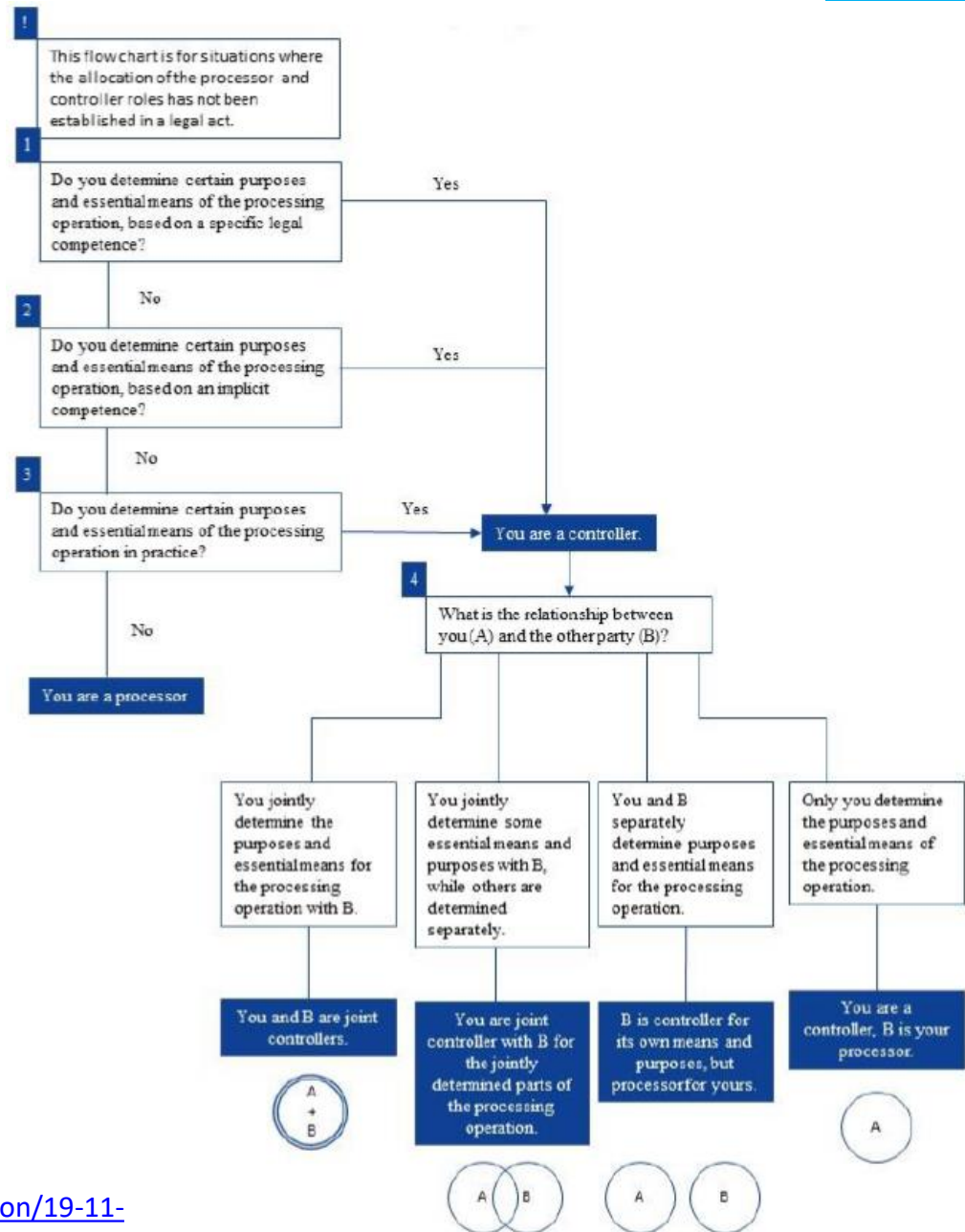
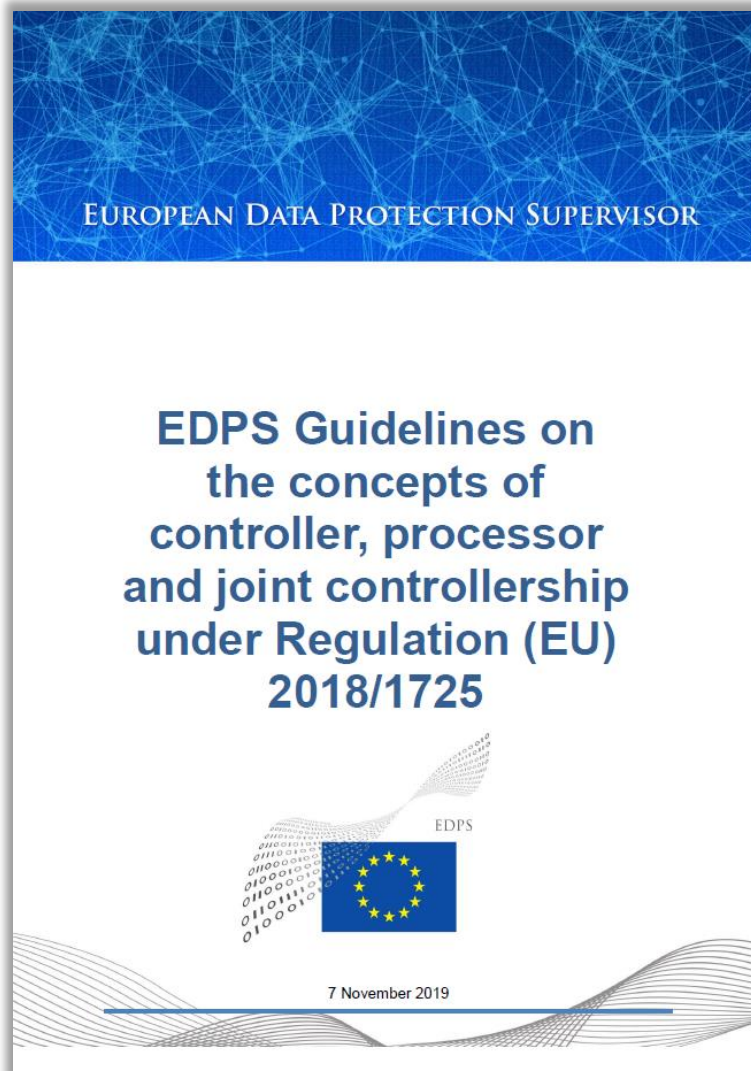



Оператор (п.2 ст.3 152-ФЗ) - ...лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных...





PART I – CONCEPTS	8
1 GENERAL OBSERVATIONS	8
2 DEFINITION OF CONTROLLER	9
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
3 DEFINITION OF JOINT CONTROLLERS	16
3.1 Definition of joint controllers	16
3.2 Existence of joint controllership	17
3.2.1 <i>General considerations</i>	17
3.2.2 <i>Assessment of joint participation</i>	18
4 DEFINITION OF PROCESSOR	24
5 DEFINITION OF THIRD PARTY/RECIPIENT	27
PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES	29
1 RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR	29
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
2 CONSEQUENCES OF JOINT CONTROLLERSHIP	40
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 <i>Form of the arrangement</i>	42
2.2.2 <i>Obligations towards data subjects</i>	43
2.3 Obligations towards data protection authorities	45





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



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:

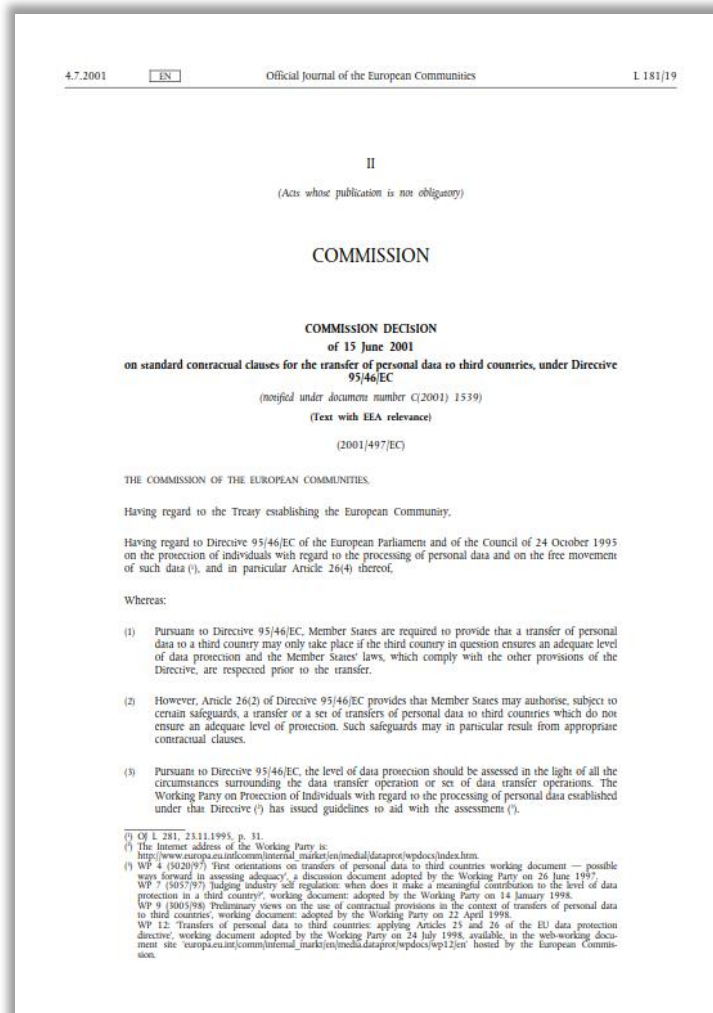
<http://sps-ib.ru/dta-eu.docx>

DPA: Standard Contractual Clauses for EU controller to non-EU or EEA processor (SCC-P)



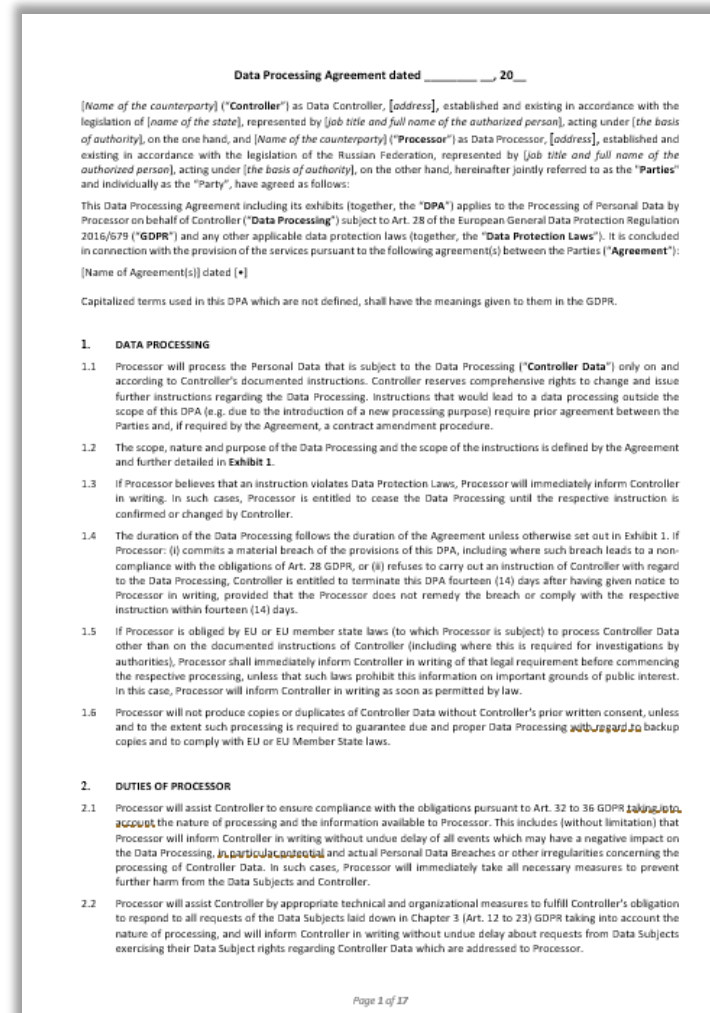
Decision 2010/87/EU

Действующая редакция устарела



<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087>

Пример DPA и интеграции в него SCC Проект подготовлен автором презентации



<http://sps-ib.ru/dpa-eu.docx>



≡ 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](#).

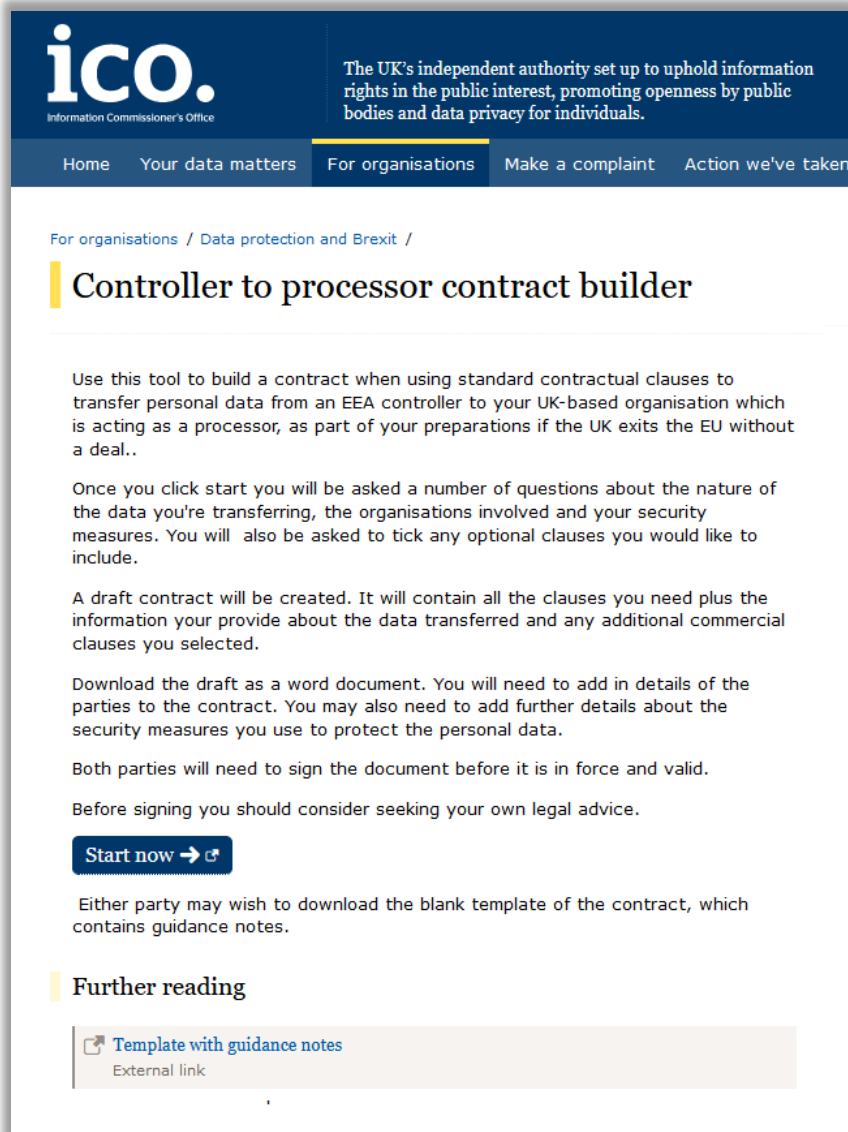
The standard processor agreement has been adopted by the Danish SA pursuant to art. 28(8) GDPR and aims at helping organisations to meet the requirements of art. 28 (3) and (4), given the fact that the contract between controller and processor cannot just restate the provisions of the GDPR but should 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.

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
PRESS RELEASE No 81/18
 Luxembourg, 5 June 2018

Judgment in Case C-210/16
 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v
 Wirtschaftsakademie Schleswig-Holstein GmbH

Press and Information

The administrator of a fan page on Facebook is jointly responsible with Facebook for the processing of data of visitors to the page

The data protection authority of the Member State in which the administrator has its seat may, under Directive 95/46,¹ act both against the administrator and against the Facebook subsidiary established in that Member State

The German company Wirtschaftsakademie Schleswig-Holstein operates in the field of education. It offers educational services inter alia by means of a fan page² hosted on Facebook at the address www.facebook.com/wirtschaftsakademie.

Administrators of fan pages, such as Wirtschaftsakademie, can obtain anonymous statistical data on visitors to the fan pages via a function called 'Facebook Insights' which Facebook makes available to them free of charge under non-negotiable conditions of use. The data is collected by means of evidence files ('cookies'), each containing a unique user code, which are active for two years and are stored by Facebook on the hard disk of the computer or on another device of visitors to the fan page. The user code, which can be matched with the connection data of users registered on Facebook, is collected and processed when the fan pages are opened.

By decision of 3 November 2011, the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent Data Protection Centre for the Land of Schleswig-Holstein, Germany), as supervisory authority within the meaning of Directive 95/46 on data protection, with the task of supervising the application in the Land of Schleswig-Holstein of the provisions adopted by Germany pursuant to that directive, ordered Wirtschaftsakademie to deactivate its fan page. According to the Unabhängiges Landeszentrum, neither Wirtschaftsakademie nor Facebook informed visitors to the fan page that Facebook, by means of cookies, collected personal data concerning them and then processed the data.

Wirtschaftsakademie brought an action against that decision before the German administrative courts, arguing that the processing of personal data by Facebook could not be attributed to it, and that it had not commissioned Facebook to process data that it controlled or was able to influence. Wirtschaftsakademie concluded that the Unabhängiges Landeszentrum should have acted directly against Facebook instead of against it.

It is in that context that the Bundesverwaltungsgericht (Federal Administrative Court, Germany) asks the Court of Justice to interpret Directive 95/46 on data protection.

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31). This directive was repealed with effect from 25 May 2018 by 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, OJ 2016 L 119, p. 1).

² Fan pages are user accounts that can be set up on Facebook by individuals or businesses. To do so, the author of the fan page, after registering with Facebook, can use the platform designed by Facebook to introduce himself to the users of that social network and to persons visiting the fan page, and to post any kind of communication in the media and opinion market.

www.curia.europa.eu

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

Tietosuojaalvautuutettu

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.

<http://curia.europa.eu/juris/celex.jsf?celex=62016CJ0210&lang1=en&type=TXT&ancre=>

<http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0025&lang1=en&type=TXT&ancre=>



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 СЛЕД 25 МАЙ 2018 Г.

10 ПРАКТИЧЕСКИ СЪТЪПКИ ЗА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ДАННИТЕ

Информационни калдосе

Начало » Практика » Становище на КЗЛД за 2018 г. » Становище на КЗЛД по искане на „УниКредит Булбанк“ АД във връзка с прилагането на Регламент (ЕС) 2016/679

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: Цветелин Софрониев, Мария Матева и Веселин Целков, 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 се поставят следните въпроси относно приложението на Регламент (ЕС) 2016/679:

1. Допустимо ли е съвместни администратори да разчитат на едно волеизявление за предоставяне на съгласие от страна на субекта, чиито данни обработват, с цел предлагане на директен маркетинг.
2. Какво качеството има банката във връзка с противоречивото тълкуване на правните фигури „администратор“ и „обработващ лични данни“ в контекста на взаимоотношенията ѝ с клиентите.

Във връзка с приваждането на дейността си в съответствие с Регламент (ЕС) 2016/679, „УниКредит Булбанк“ АД се сблъсква с противоречиво тълкуване от страна на своите клиентинакачеството на страните в отношенията, свързани с предоставянето 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, визирайки, че банката има качеството на обработващ данните. Основният им аргумент в тази насока е, че сключваните между странитедоговори 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“ АДне 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 качествотоизадълженията на „администратор“ на собствено основание по отношение на събираните и обработваните личниданни.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.

търсене

Политика за прозрачност

Годишни отчети

Информационен бюлетин

Профил на купувача

Административно обслужване

Медии

Съобщения

Информационна кампания

По жалби

Търгове

Календар на събитията

Ноември 2018

П	В	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

Конференция 2015

Конкурс за деца

Наредба № 1 от 30 януари 2013 – отменена, считано от 25.05.2018

Списъци, свързани с

Комисията за защита на личните данни

Болгарский надзорный орган КЗЛД опубликовал свой ответ на запрос банка «УниКредит Булбанк», в котором рекомендует заключать соответствующий договор между совместными контролерами. В договоре должны быть определены обязанности каждой стороны по соблюдению требований GDPR (особенно в отношении механизма реализации прав субъектов данных и обязательств по уведомлению субъектов). Кроме того, информация о факте заключения такого договора и его содержание должны быть доведены до сведения субъектов данных.

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.

Vereinbarung gemäß Art. 26 Abs. 1 S. 1 Datenschutz-Grundverordnung (DS-GVO) zwischen

Partei 1

[Name und Kontaktdaten angeben]

und

Partei 2

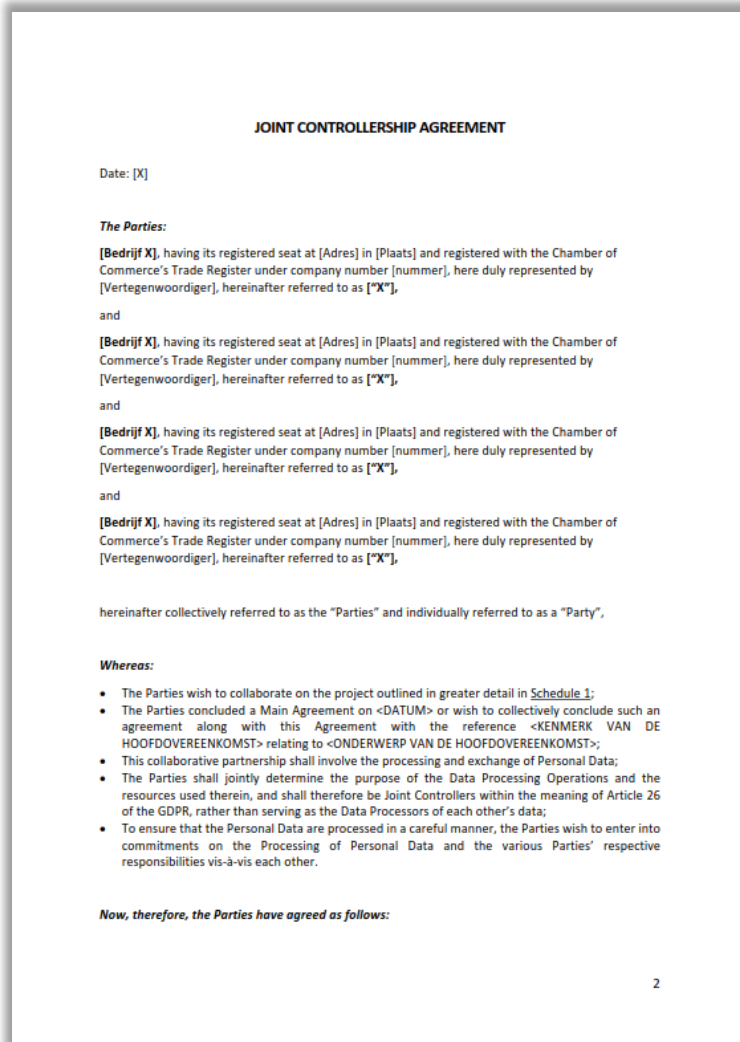
[Name und Kontaktdaten angeben]

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.



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.

Model Joint Controllership Agreement of SURF:
<https://www.surf.nl/files/2019-11/model-joint-controllership-agreement.pdf>



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. [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](#)
2. [Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264](#)
3. [Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265](#)
4. [Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01](#)
5. [Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01](#)



Некоторые из компаний-участников BCR:

- | | | |
|---------------------|-------------------|--------------------|
| 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 |

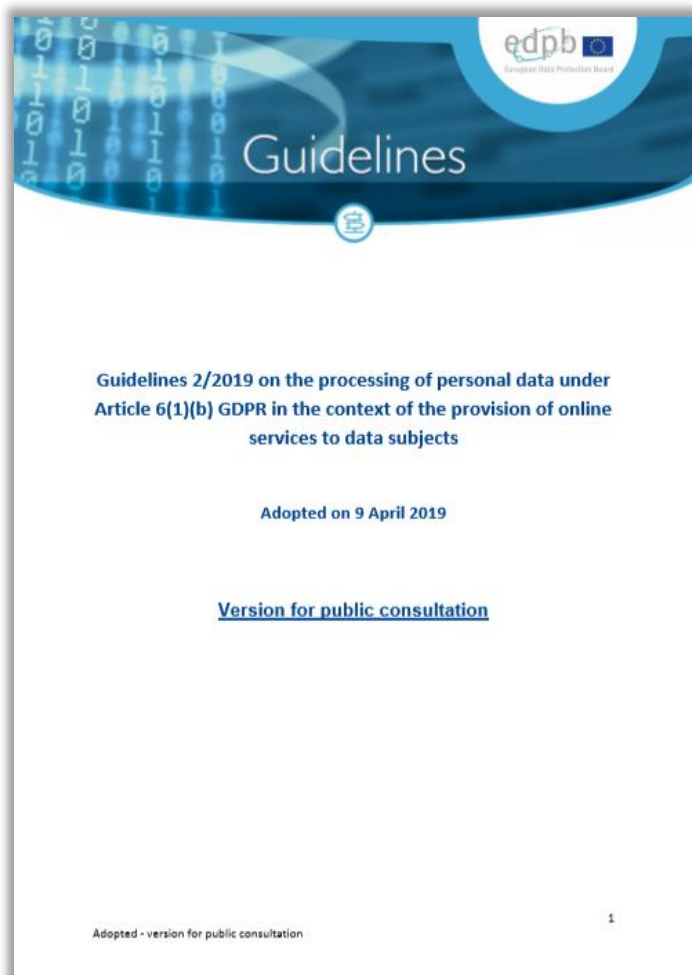


Некоторые из компаний-участников BCR:

- Equinix (2019)
- ExxonMobil (2019)
- Fujikura Automotive Europe Group (2020)

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841

https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en



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).

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
Contract	✓	✓	✓	✓	✓	✗
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)

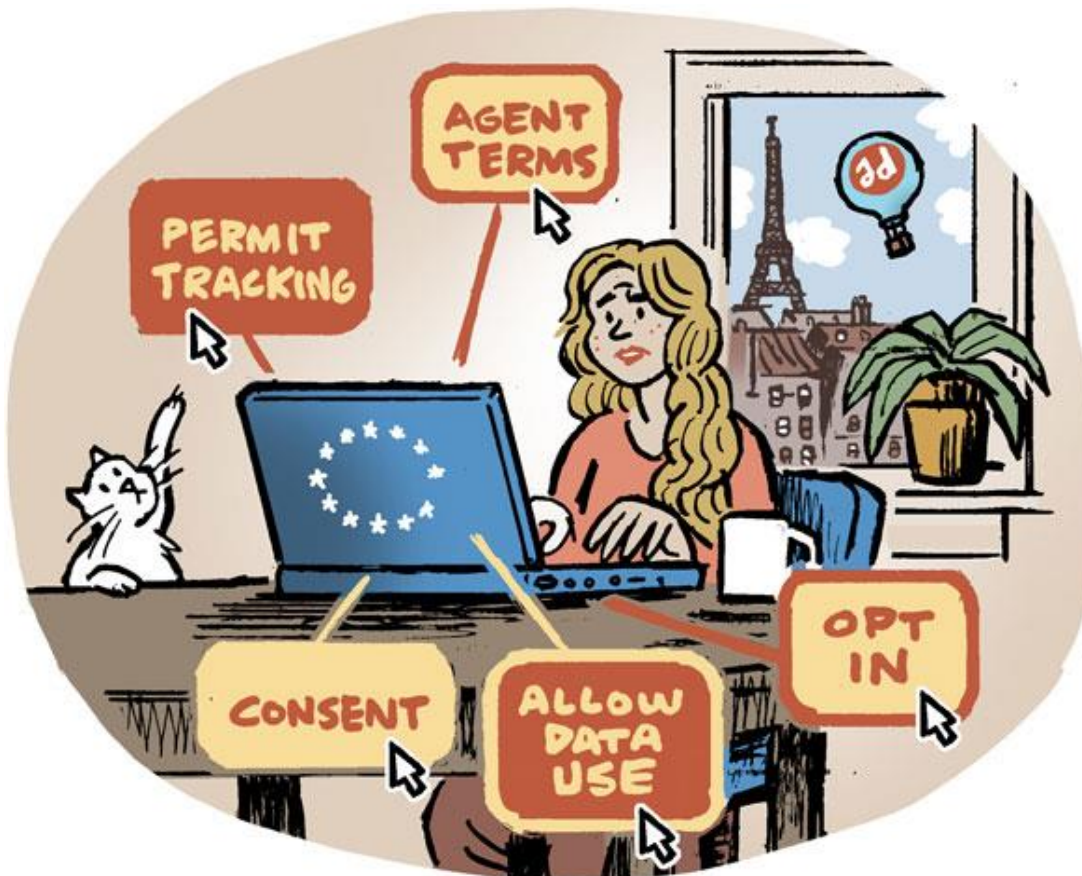
1. Подписывая Договор, Исполнитель наделяет Заказчика, как самостоятельно действующего оператора (здесь и далее понятия «оператор», «персональные данные», «обработка персональных данных» используются в значении, определенном ст.3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»), правом 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.

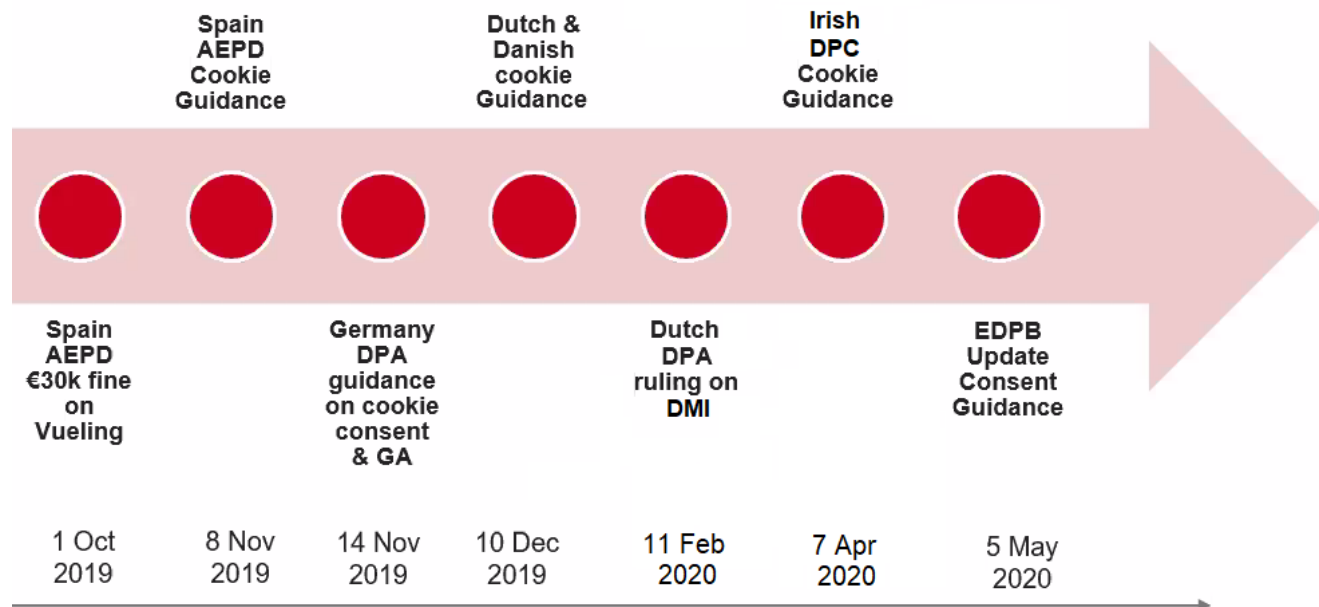
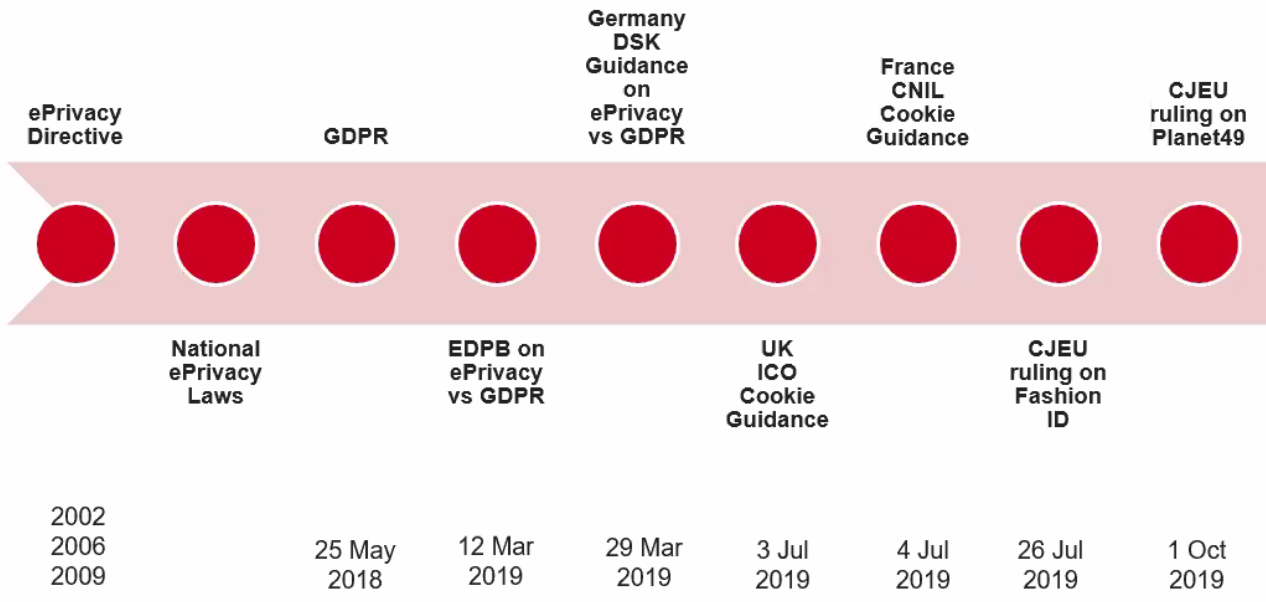
- ✓ определяет статус организации в отношении с субъектом данных как самостоятельного контролера;
- ✓ фиксирует цели договорной обработки персональных данных – заключение, исполнение и прекращение сторонами договора, а также осуществление, выполнение и соблюдение Сторонами прав, обязанностей и запретов, 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.

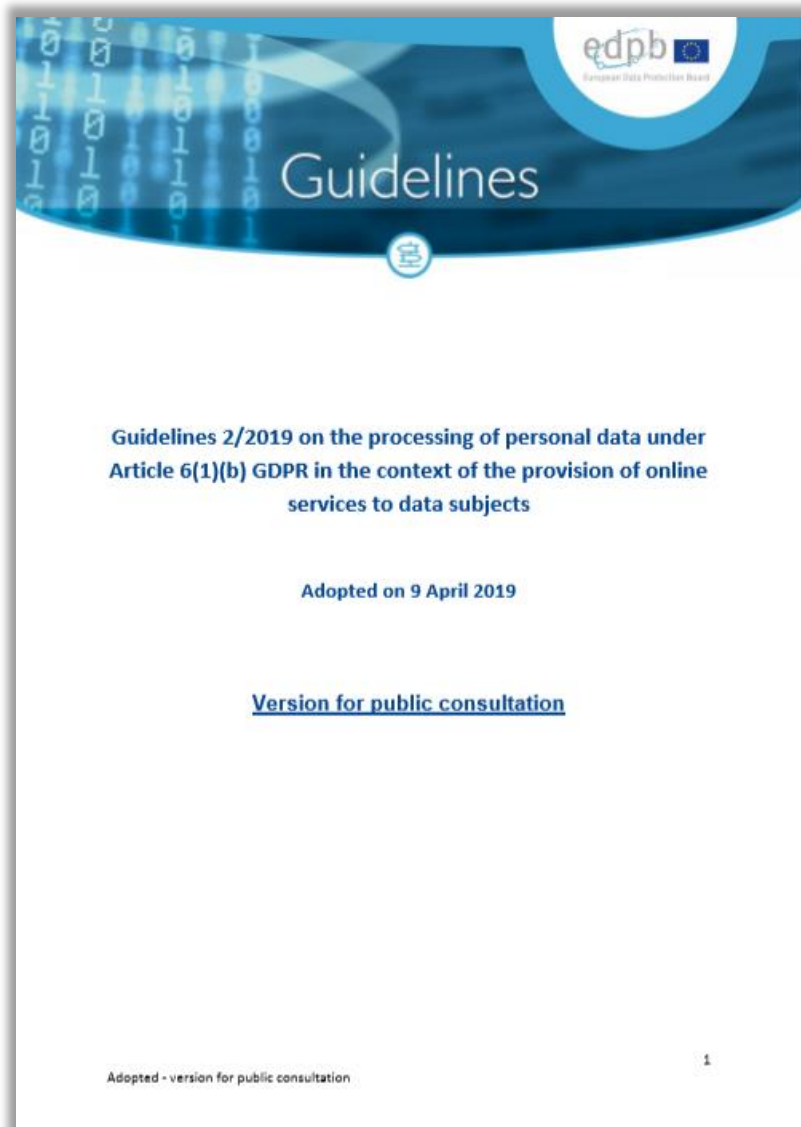
Подготовленный автором презентации проект SPA, предназначенный для **договоров согласно праву РФ:**

<http://sps-ib.ru/spa.docx>

Взаимодействие с пользователями сайтов и приложений







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.

- ✓ 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.*



The screenshot shows the ICO website's guidance page. 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." The navigation menu includes: Home, Your data matters, For organisations (selected), 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 is divided into sections:

- About this guidance**
 - 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?
 - What else do we need to consider?
- Contents**
 - 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.



**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).



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 Commission nationale de l'informatique et des libertés (CNIL) 17.09.2020 года принял новую редакцию руководства по использованию файлов cookie, согласно которому:

- стены 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.



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.

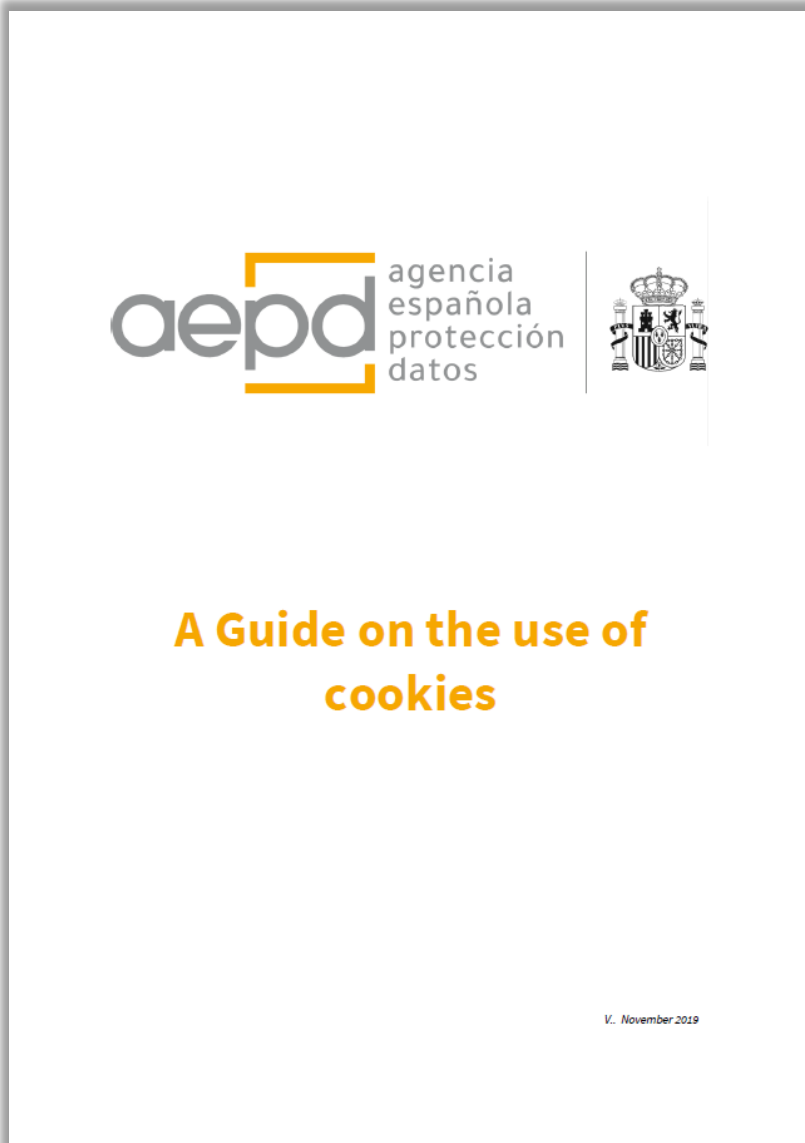
Det er efter Datatilsynets opfattelse i strid med det grundlæggende princip om gennemsigtighed.

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.



Example no. 1:

COOKIES

We use our own and third-party cookies to analyse our services and show ads related to your preferences, according to profiling based on your browsing habits (for example, websites visited). You may know more and set up your preferences: [HERE](#).

ACCEPT COOKIES

REJECT COOKIES

Example no. 2:

We use our own and third party cookie for analytic purposes and in order to show personalised ads according to profiling based on your browsing habits (for example, websites visited). Click [HERE](#) to know more. You may accept all cookies by clicking on "Accept" or reject or set up your preferred configuration by clicking [HERE](#).

ACCEPT

Example no. 3:

COOKIES

We use our own and third party cookie for analysing our own services and to show ads which are relevant for you according to profiling based on your browsing habits (for example, websites visited). If you continue browsing, we will consider that you accept them. You may reject or set up your preferred configuration by clicking [HERE](#).

Example 1:

If you are under 14 years of age, please ask your father, mother or tutor to read this message.

We use both our own and third-party cookies to find out how you use our website and prepare statistical surveys. [More information](#).

Your father, mother or tutor may press "Accept" if he or she agrees with us using all cookies. He or she may also set up or refuse these cookies [HERE](#).

ACCEPT

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	

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.

Проблема	Позиция ICO, CNIL и AP
Согласие	<p>Подразумеваемое согласие недостаточно - требуется явно выраженное согласие согласно требованиям GDPR</p> <p>Организации должны иметь возможность продемонстрировать получение согласия в надлежащей форме</p>
Стены cookie	Не признаются правомерными
Технические cookies	Согласие не требуется
Аналитические cookies	<p>ICO: согласие требуется</p> <p>CNIL: согласие не требуется при определенных условиях</p> <p>AP: согласие не требуется при определенных условиях</p>
Демонстрация прозрачности	Повышенные требования к информированности пользователей

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?
Austria	No.	Unclear, but likely no.	Yes (currently).	Unclear, but likely no.	Ireland	No.	No.	No.	No.
Belgium	Yes – 1 fine.	No.	No.	No.	Latvia	No.	No.	No.	No.
Bulgaria	No.	Unclear – no specific rules or guidance.	No.	No.	Lithuania	No.	Unclear, although it is unlikely (see guidance).	No.	No.
Croatia	No.	No.	Unclear.	No; however, see additional guidance for exceptions.	Luxembourg	No.	Yes.	No.	No (see additional guidance for exceptions).
Cyprus	No.	No.	No.	No.	Malta	No.	Unclear.	Unclear.	Unclear.
Czech Republic	No.	Yes; however, see additional guidance for details.	No.	Yes; however, see additional guidance for details.	Netherlands	Yes.	No.	No.	No.
Denmark	No.	No.	No.	No.	Norway	No.	No.	No.	No.
Estonia	No.	No.	No.	No.	Poland	No.	Yes.	Unclear; however, unlikely (see additional guidance).	No.
Finland	Yes – 1 case.	No.	Unclear, although it is unlikely (see additional guidance).	No.	Portugal	No.	No.	No.	No.
France	Yes – 3 fines, 3 court cases.	No.	Unclear, assessed on a case-by-case basis (see additional guidance).	No.	Romania	No.	Yes.	Unclear (see additional guidance).	No.
Germany	Yes – 1 case.	No.	Unclear (see additional guidance)	Unclear (see additional guidance)	Slovak Republic	No.	Yes.	No.	Yes.
Hungary	No.	No.	No.	No.	Slovenia	No.	Unclear (see additional guidance).	No.	No.
Italy	No.	Yes.	Unclear; however, unlikely (see additional guidance).	Yes.	Spain	Yes, 41 fines on non-compliance since 2014.	Yes; however, see additional guidance for details on limitations.	Unclear (see additional guidance).	Yes.
					Switzerland	No.	Yes.	Unclear (see additional guidance).	Yes.
					UK	No.	No.	No.	No.



Блоки взаимоотношений

Способы взаимодействия

Формализация взаимоотношений

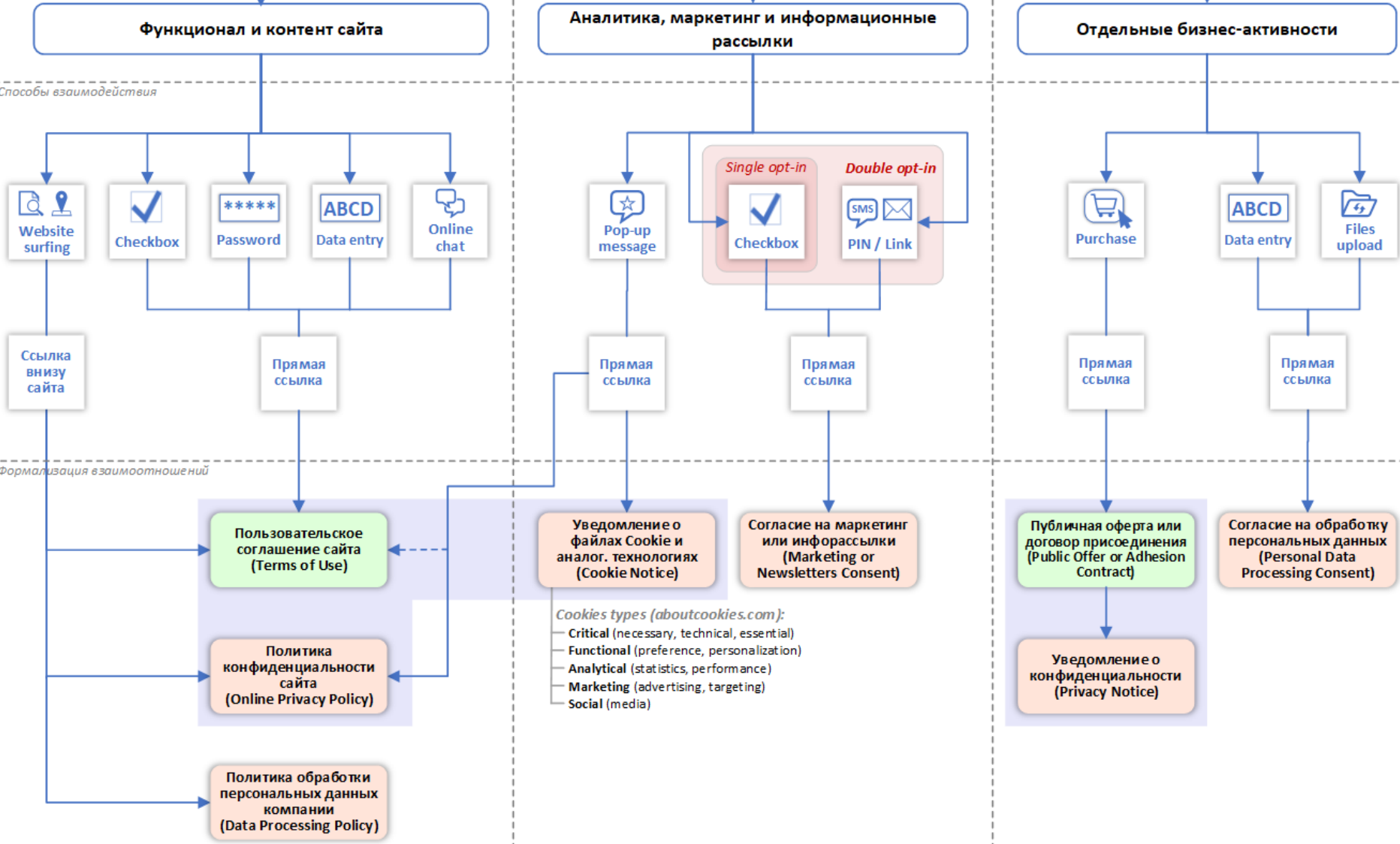




Table 1: cookies used by commonly used website

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

Импорт данных в Google Analytics - https://support.google.com/analytics/topic/6065609?hl=ru&ref_topic=1727148



Are cookie banners indeed compliant with the law?

Cristiana Santos, Nataliia Bielova, Célestin Matte

► To cite this version:

Cristiana Santos, Nataliia Bielova, Célestin Matte. Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. 2020. hal-02875447v2

HAL Id: hal-02875447

<https://hal.inria.fr/hal-02875447v2>

Preprint submitted on 23 Sep 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Table 6 Requirements for a valid consent on consent banner design, assessment and source

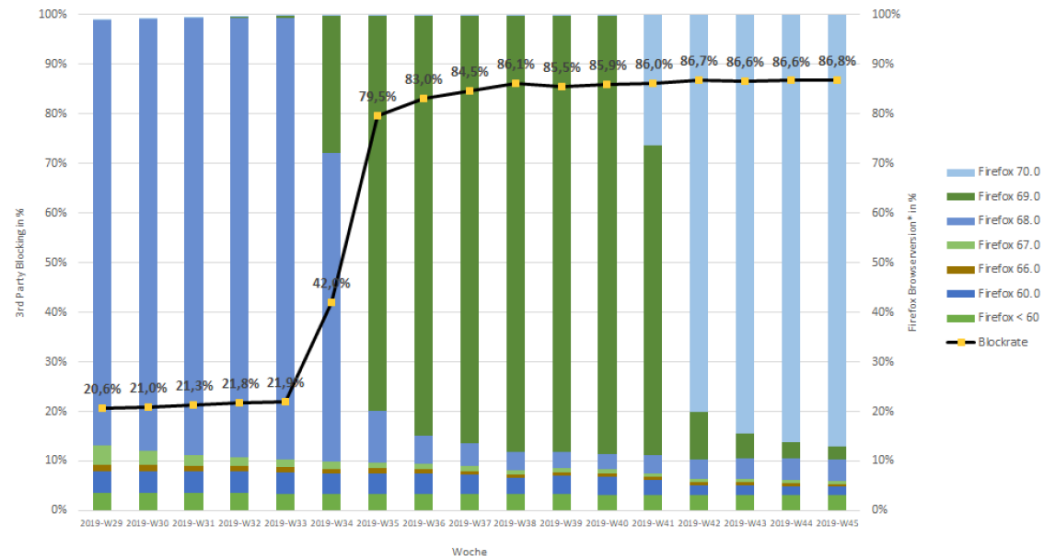
Requirements		Assessment	Sources at low-level requirement			Location in the paper (page)
High-Level Requirements	Low-Level Requirements	Manual (M), Technical (T) or User study (U)	Binding	Non-binding	Interpretation: Legal (L) or Computer Science (CS)	
Prior	R1 Prior to storing an identifier	M (partially) 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

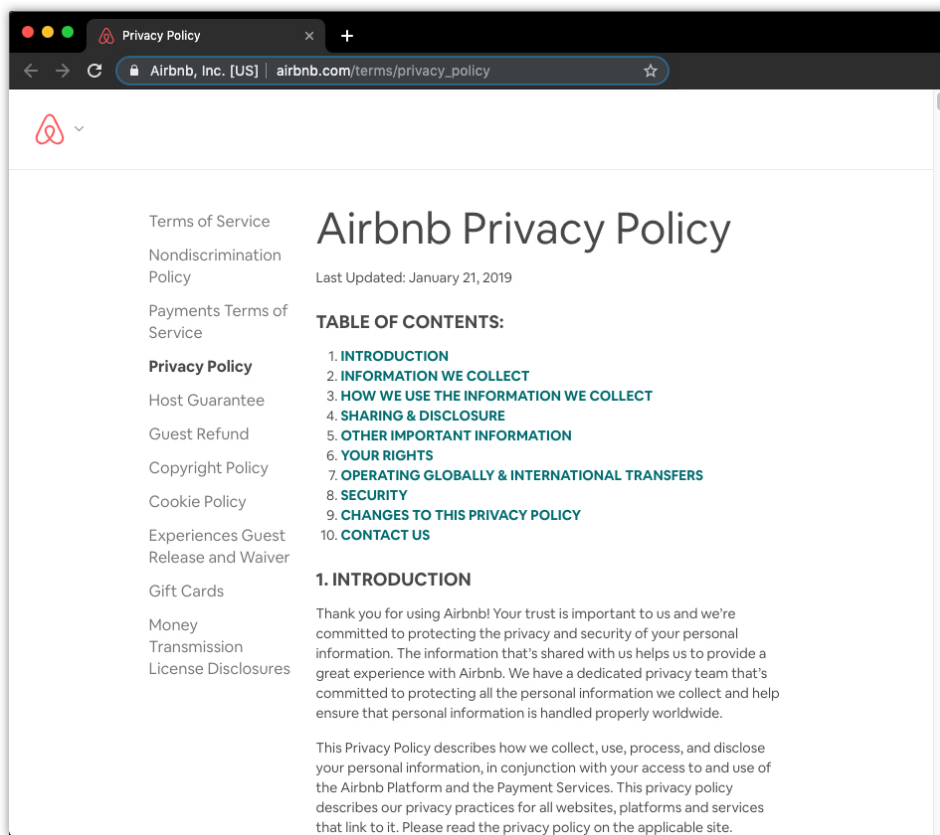


Европейское бюро интерактивной рекламы (Interactive Advertising Bureau - IAB) 7 мая 2020 г. опубликовало Руководство по эре, наступающей после отказа от использования сторонних файлов cookie (Guide to the Post Third-Party Cookie Era). В руководстве рассматриваются факторы, способствующие отказу от использования 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.

Monitoring Firefox Enhanced Tracking Prevention

Die Firefox-Browserversionen wurden über den UserAgent aus den WebAnalytics-Daten ermittelt. In die Auswertung gehen alle FF-Versionen ein, mit denen 97% der PIs in den letzten 90 Tagen generiert wurden. Die Blockrate wird über eine Ad-ID-Kampagne auf einem TAM-Werbepplatz der Homepage gemessen. Bei dieser Kampagne wurden direkte und indirekte AdBlocker ausgeschlossen. Verschiedene Adserver-Events ermitteln, ob bei einer Ad-ID eine Cookie-ID vorliegt und um welche Browserversion es sich handelt. Ab KW31 wurde eine neue Messung eingeführt, weshalb für die KWs 29 und 30 keine validen Zahlen vorliegen.





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.

The screenshot shows the Cookiebot website with a blue header. The main heading is "Is my website compliant?". Below it, there is a paragraph explaining GDPR and ePrivacy compliance. At the bottom, there is a search bar for "Your website address" and a "CHECK MY WEBSITE" button.

<https://www.cookiebot.com/en/>

The screenshot shows the CookiePro website with a blue header. The main heading is "Cookie Consent & Website Scanning". Below it, there is a search bar for "Enter your domain name" and a "SCAN" button.











<https://www.cookiepro.com/products/cookie-consent/>

The screenshot shows the OneTrust website with a green header. The main heading is "Cookie Consent and Website Scanning". Below it, there is a paragraph explaining GDPR and ePrivacy compliance. At the bottom, there is a grid of six icons representing various features and statistics.

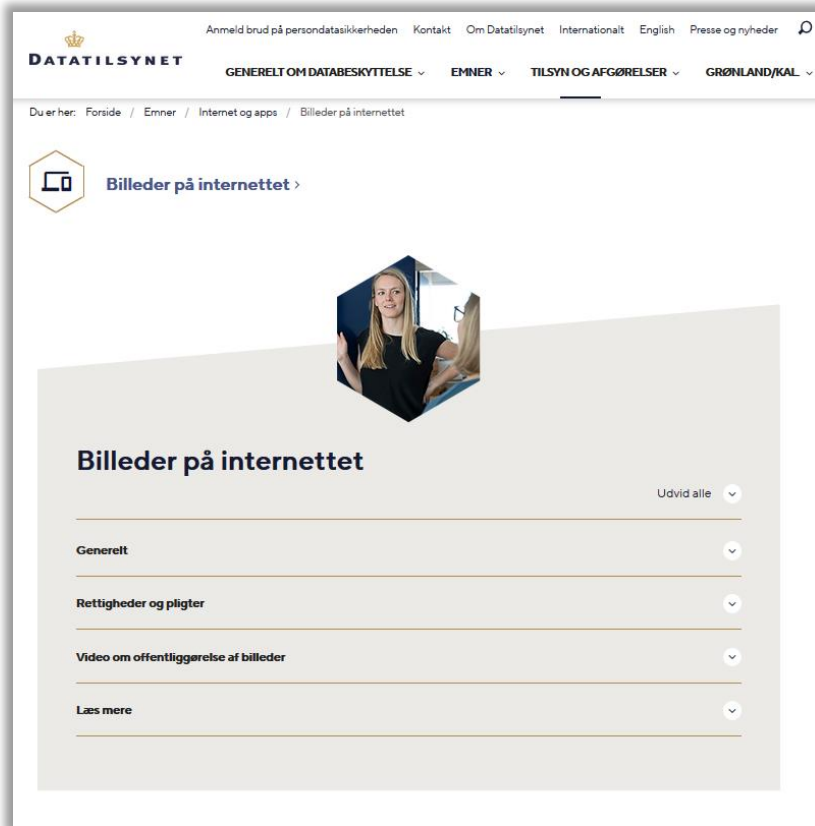
<https://www.onetrust.com/products/cookies/>

The screenshot shows the Termly website with a white header. The main heading is "GDPR Cookie Consent Manager". Below it, there is a paragraph explaining the service. At the bottom, there is a "Start Building Cookie Consent" button and a grid of icons representing various integrations.

<https://termly.io/products/cookie-consent-manager/>

App	Summary of findings
 Clue	Sends birth year to Amplitude , Apptimize , and Braze . Sends Advertising ID to Adjust , Amplitude , and Facebook .
 Grindr	Sends GPS coordinates to AdColony , Braze , Bucksense , MoPub , OpenX , Smaato , PubNative , Vungle , and others. Sends the IP address to AppNexus and Bucksense , and information about "relationship type" to Braze . Sends Advertising ID to all of these third parties and others, except Braze .
 Happn	Sends country, gender and age segment of the user to Google . Sends Advertising ID to Adjust and Facebook .
 Muslim: Qibla Finder	Sends IP address to Appodeal . Sends Advertising ID to AppLovin , Appodeal , Facebook , and Liftoff .
 My days	Sends GPS coordinates and Wi-Fi access point information to Neura , Placed , and Placer . Sends IP address and a list of installed apps on the phone to Placed . Sends Advertising ID to AppLovin , Liftoff , Google , Ogury Presage , and Placed .
 My Talking Tom 2	Sends IP address to Mobfox , PubNative , and Rubicon Project . Sends Advertising ID to AppsFlyer , AppLovin , Facebook , IQzone , ironSource , Mobfox , Outfit7 , and Rubicon Project .
 OkCupid	Sends GPS coordinates and answers to personal questions to Braze . Sends detailed device information to AppsFlyer . Sends Advertising ID to AppsFlyer , Facebook and Kochava .
 Perfect365	Sends various location data such as GPS coordinates and Wi-Fi access point information to Fysical , Safegraph , and Vungle . Sends GPS coordinates unencrypted to Receptiv . Sends Advertising ID to Amazon , Chocolate , Facebook , Fluxloop , Fyber , Fysical , InMobi , Inner-Active , Ogury Presage , Safegraph , Receptiv , Unacast , Unity3d , and Vungle .
 Tinder	Sends GPS position and "target gender" to AppsFlyer and LeanPlum . Sends Advertising ID to AppsFlyer , Branch , Facebook , and Salesforce (KruX) .
 Wave Keyboard	Sends Advertising ID to Crashlytics , Facebook , Flurry , OneSignal .

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.



Датский надзорный орган Datatilsynet пересмотрел свои разъяснения от 2002 года относительно обработки персональных данных при публикация 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.

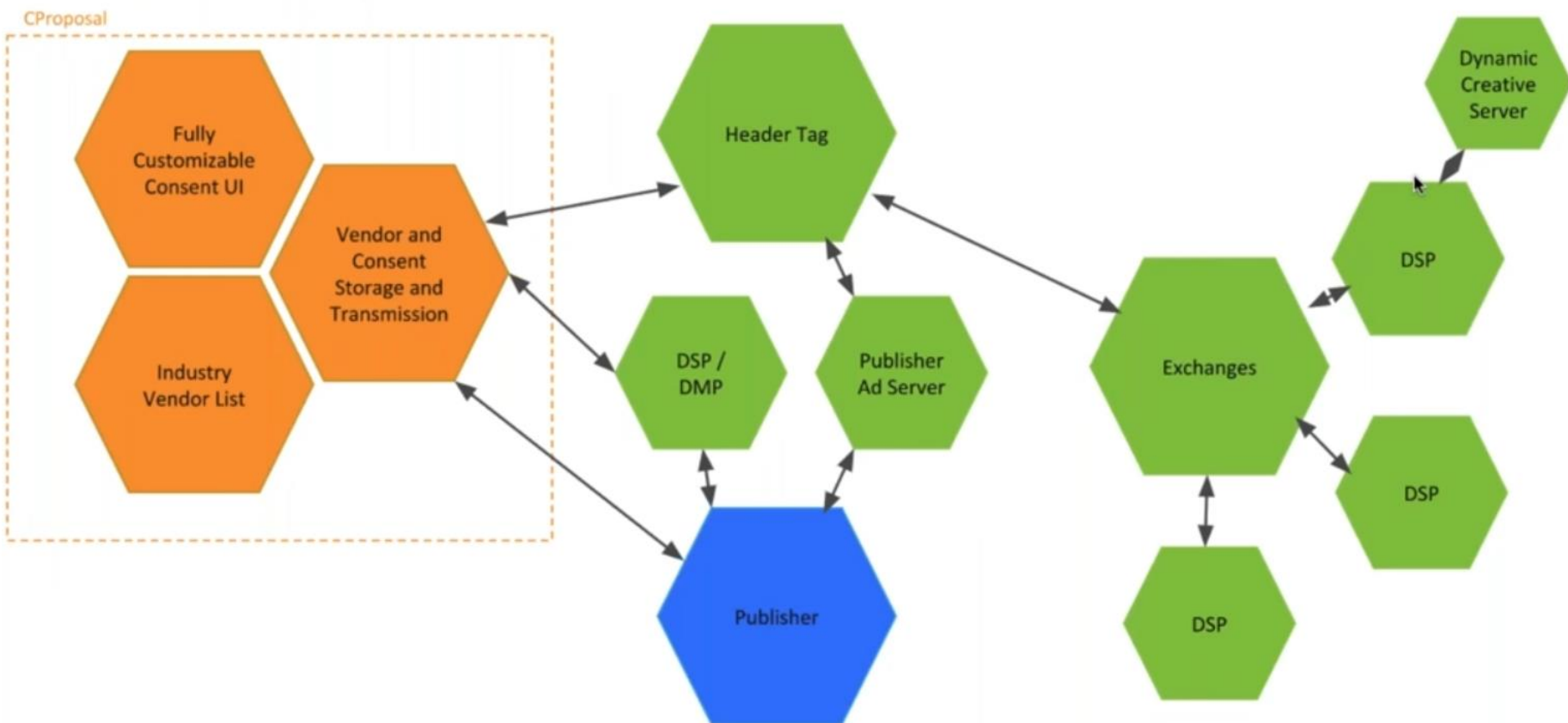
На этом фоне Датское агентство по защите данных решило изменить свою практику и больше не проводить различие между ситуативными и портретными изображениями, а далее – оценивать вопрос о публикации фотографии субъекта данных (без его согласия) в Интернете на основании всесторонней оценки изображения и цели публикации.



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.

182 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).





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

UN OFFICIAL TRANSLATION by Christopher Schmidt, CIPP/E CIPM CIPT CBSA

	Discord	FaceTime	Hangouts Google	Hangouts Meets Google	Houseparty	Jitsi	Messenger Facebook	Signal	Skype	Talk Microsoft	Teams Microsoft	WhatsApp	Zoom*
What does the app offer?													
(group) chat (text)	1	1	1	1	1	1	1	1	1	1	1	1	1
1-to-1 calls (audio and/or video)	1	1	1	1	1	1	1	1	1	1	1	1	1
group calls (audio and/or video)	1	1	1	1	1	1	1	1	1	1	1	1	1
set up and manage yourself (self-hosted)													
participation in conversation w/o creating an account									2	2	2		2
use in browser					3							4	
use on different platforms (cross-platform)					5							6	7
What data does the app collect?													
address book		8	8	8	8						9	8	
location data													
call data	10		10	10	10								
metadata	10		10	10	10								
linking data with data from other products or profiles												11	12
For what purposes does the app process data?													
For using the app	13	13	13	13	13	13	13	13	13	13	13	13	13
For improving the app	14	14	14	14	14	14	14	14	14	14	14	14	14
Show (personalised) advertisements	15	15	15	15	15	15	15	15	15	15	15	15	15
How does the information flow look like?													
Data Processing Agreement possible						16							
Data transfer to 3rd parties (if so, what data and to whom)	16	16	16	16	16	16	16	16	16	16	16	16	16
Location of data controller	17	17	17	17	17	17	17	17	17	17	17	17	17
data remain in the Netherlands													
data remain in the EU													
Is the communication secure?													
end-to-end encryption (even the provider of the app cannot access the content of the communication)							18			18			
encryption of traffic during transfer, so that third parties cannot access it (note: the provider of the app may be able to access it, but this does not mean it will happen).							19			19			
minimisation of metadata use							20			20			
encryption by default							21			21			
anyone can check source code (open source)							22			22			
How does the app make money?													
paid subscription or paid version	23	23	23	23	23	23	23	23	23	23	23	23	23
(personalised) advertisements	24	24	24	24	24	24	24	24	24	24	24	24	24
donations													
otherwise							25					25	
Where can you find information?													
privacy statement (refer to the Dutch original for clickable link)	26	26	26	26	26	26	26	26	26	26	26	26	26
privacy statement in Dutch	27	27	27	27	27	27	27	27	27	27	27	27	27

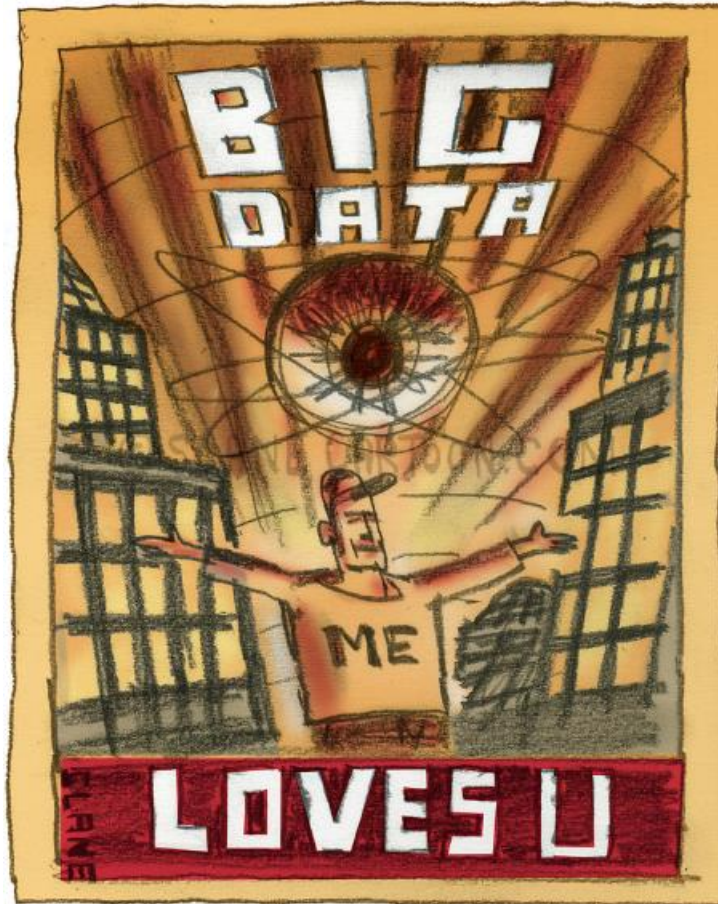
- Video only
- After installation
- Google Chrome
- Skype for Web in Microsoft Edge or Google Chrome
- Not for video or audio
- Android, iOS, Google Chrome
- Mobile/desktop
- With other Facebook products
- Please note: when calling via website
- N/A (self-hosted)
- Standard agreement
- For some sectors
- Metadata and IP data for business purposes, but no sale of data
- To Apple Subscribers and Agents
- Within Google
- To public authorities when they so request and to related companies
- Within Facebook and to external partners
- To public authorities when they so request
- Within Microsoft
- To Facebook and to third parties, but not (yet) for advertising purposes within Facebook
- To supporting partners, but no sale of data
- Not for (video) calling for chatting you have to start this separately in Secret Mode
- Only in private conversations (see: [website](#))
- In group discussions
- Discord Nitro
- Supplied as standard for new Apple products
- Skype for Business
- The enterprise edition has been paid for
- There are several subscriptions, but also a free version
- Please note: when calling via website
- Project is fully supported by the company itself
- Not of Facebook
- This depends on the person offering a Nextcloud service

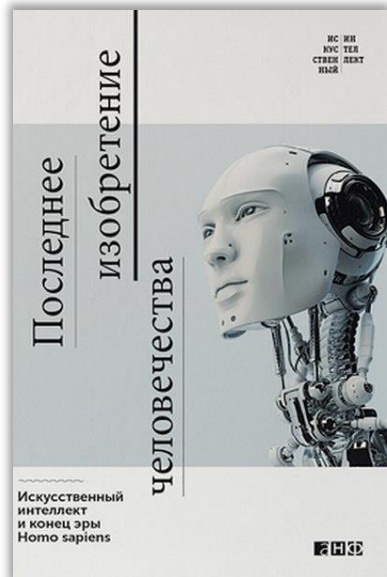
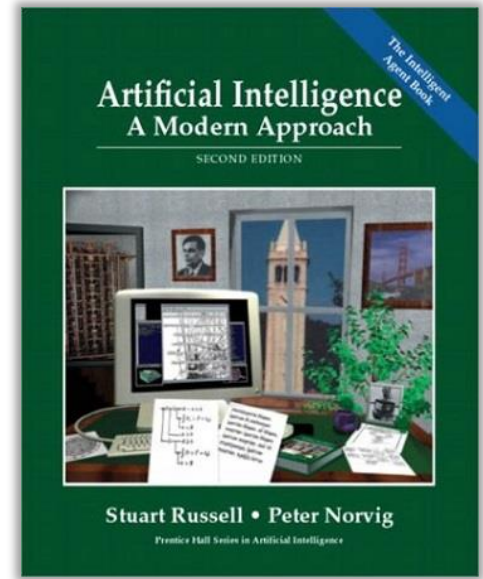
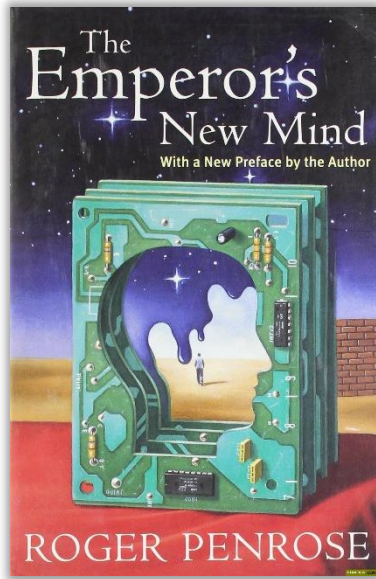
* Be careful when using Zoom, this app is still in development.
 ** Note: For group calls, there is either no end-to-end encryption, or only with a limited number of participants.
 Please note that the AP has not been able to do extensive technical research on the apps. The AP relies on what companies say about how video call apps process your data, for example in their privacy statement.

<https://autoriteitpersoonsgegevens.nl/nl/nieuws/keuzehulp-privacy-bij-videobel-apps>

<https://workupload.com/file/8FzuCsSkMky>

Большие данные, искусственный интеллект и машинное обучение





“...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>

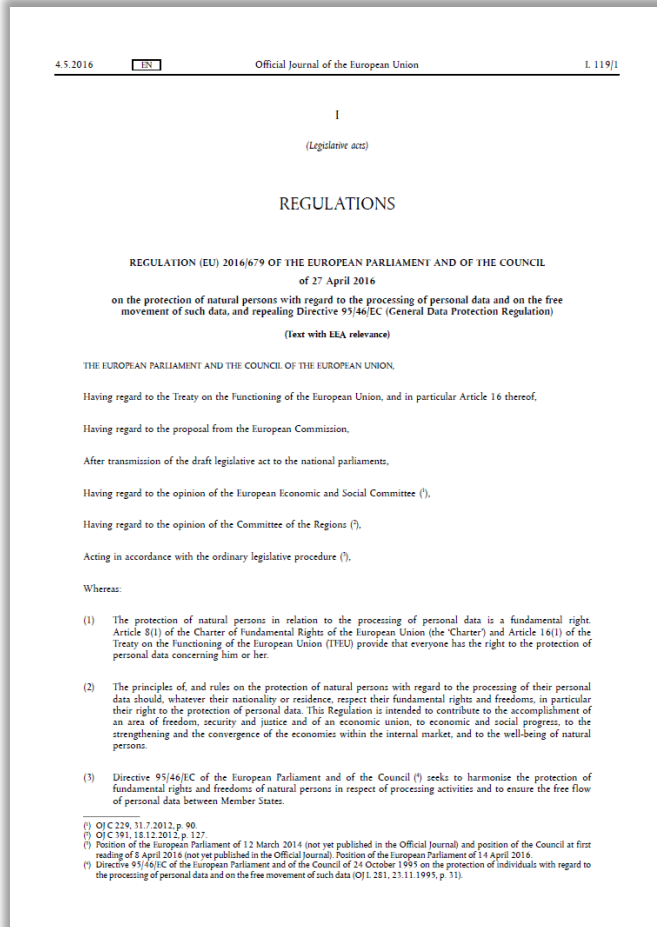
“A set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being. Current developments aim, for instance, to be able to entrust a machine with complex tasks previously delegated to a human.”

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 (STOA)
PE 641.530 – June 2020

EN

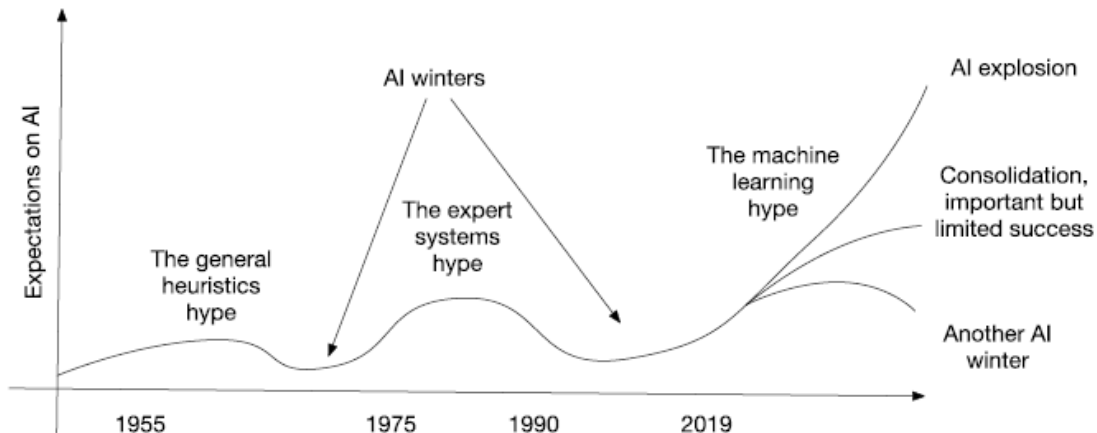


Figure 1 – Hypes and winters of AI

2018 This Is What Happens In An Internet Minute



2019 This Is What Happens In An Internet Minute



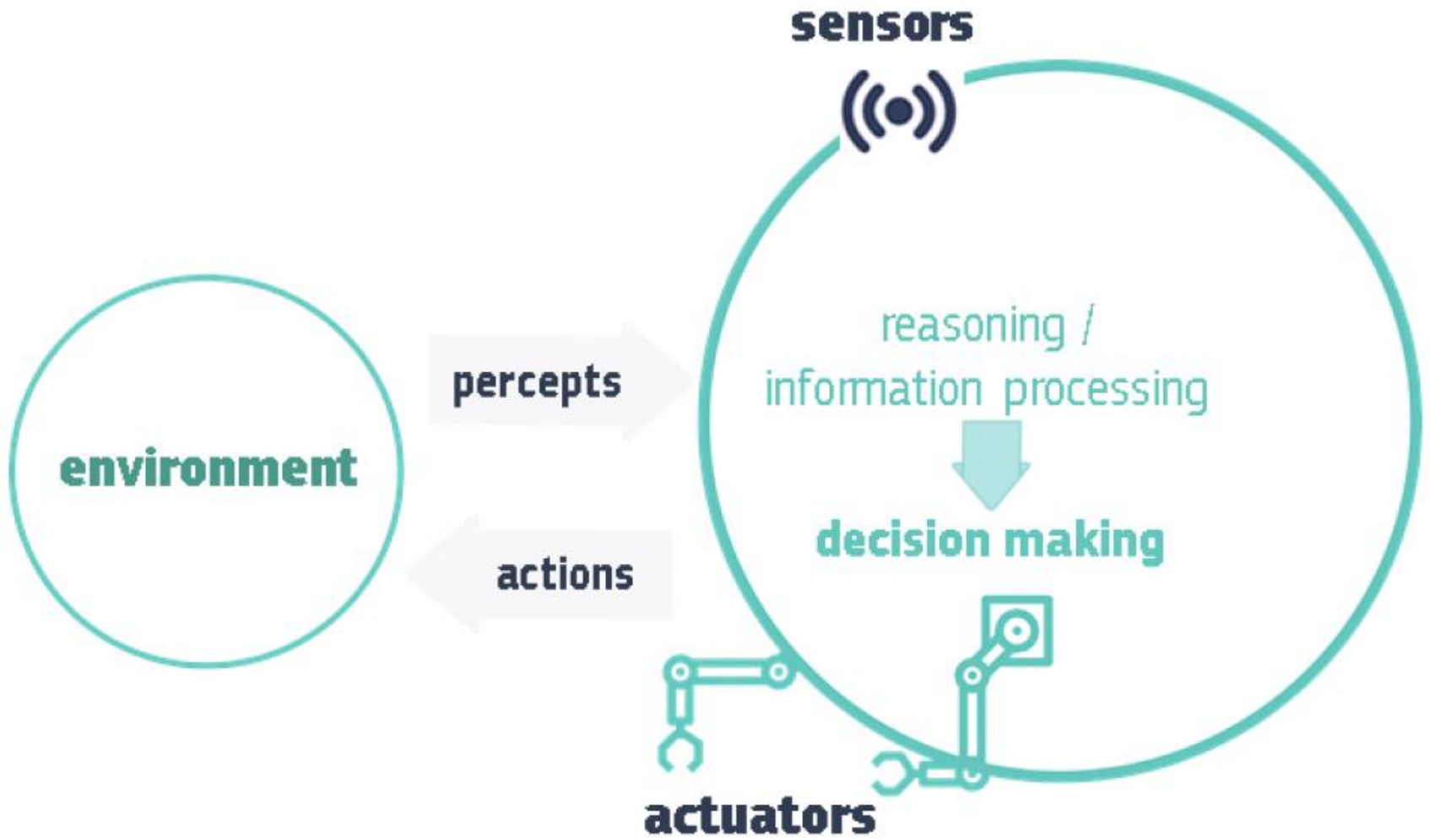
Figure 10 – Data collected in a minute of online activity worldwide

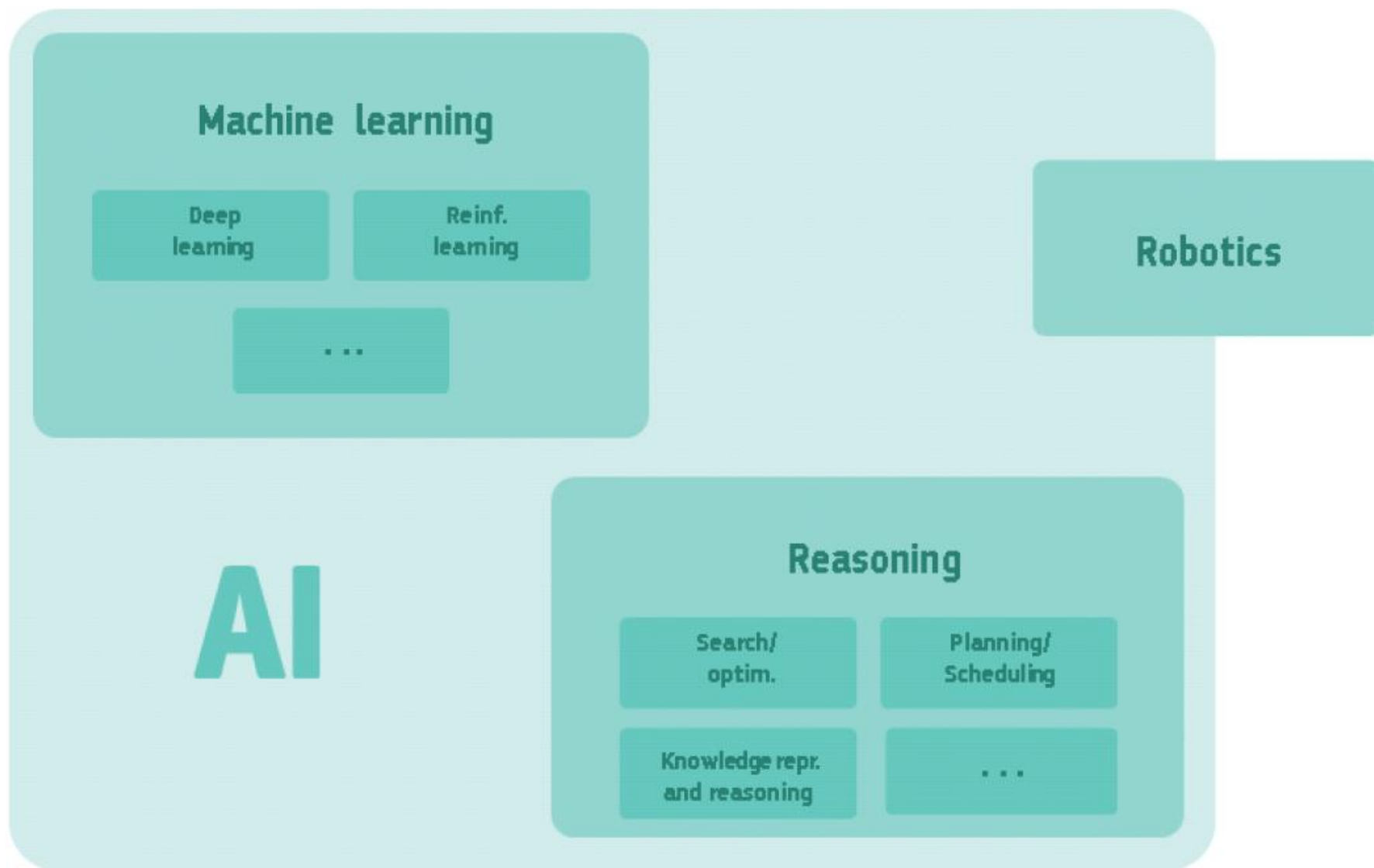


В докладе отмечается важность обсуждения и понимания всех типов угроз ИИ до начала его повсеместного развертывания, а также сертификации безопасности систем ИИ.

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.







Brussels, 19.2.2020
COM(2020) 65 final

WHITE PAPER

On Artificial Intelligence - A European approach to excellence and trust

Artificial Intelligence is developing fast. It will change our lives by improving healthcare (e.g. making diagnosis more precise, enabling better prevention of diseases), increasing the efficiency of farming, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the security of Europeans, and in many other ways that we can only begin to imagine. At the same time, Artificial Intelligence (AI) entails a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes.

Against a background of fierce global competition, a solid European approach is needed, building on the European strategy for AI presented in April 2018¹. To address the opportunities and challenges of AI, the EU must act as one and define its own way, based on European values, to promote the development and deployment of AI.

The Commission is committed to enabling scientific breakthrough, to preserving the EU's technological leadership and to ensuring that new technologies are at the service of all Europeans – improving their lives while respecting their rights.

Commission President Ursula von der Leyen announced in her political Guidelines² a coordinated European approach on the human and ethical implications of AI as well as a reflection on the better use of big data for innovation.

Thus, the Commission supports a regulatory and investment oriented approach with the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of this new technology. The purpose of this White Paper is to set out policy options on how to achieve these objectives. It does not address the development and use of AI for military purposes. The Commission invites Member States, other European institutions, and all stakeholders, including industry, social partners, civil society organisations, researchers, the public in general and any interested party, to react to the options below and to contribute to the Commission's future decision-making in this domain.

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



www.coe.int/data-protection



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.

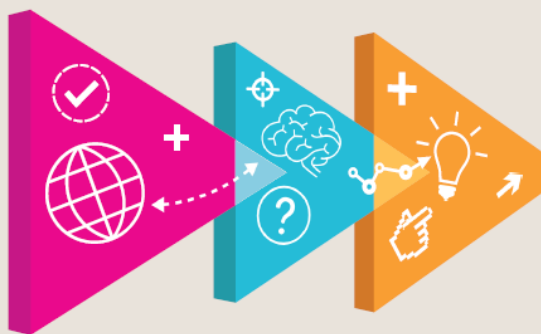


Big data, artificial intelligence, machine learning and data protection

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.

Guidance on the AI auditing framework

Draft guidance for consultation

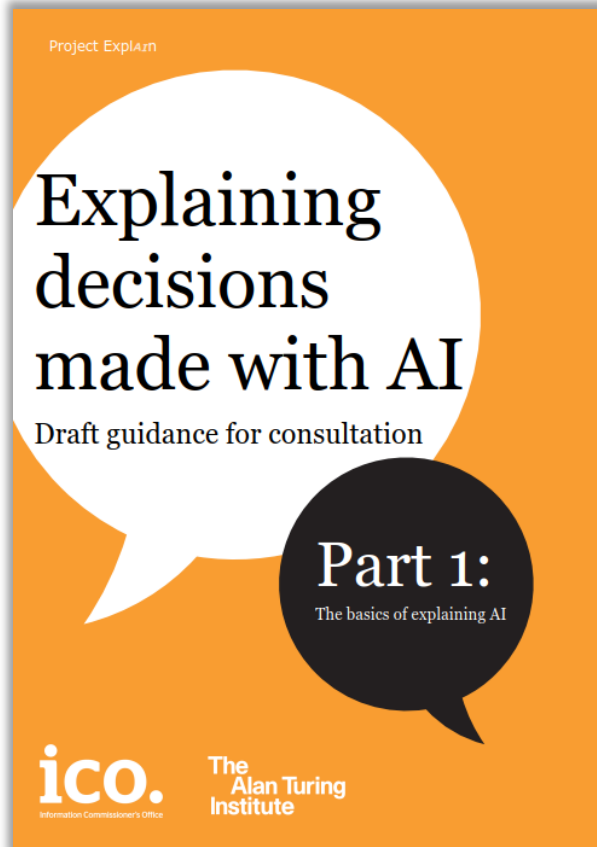


ico.
Information Commissioner's Office

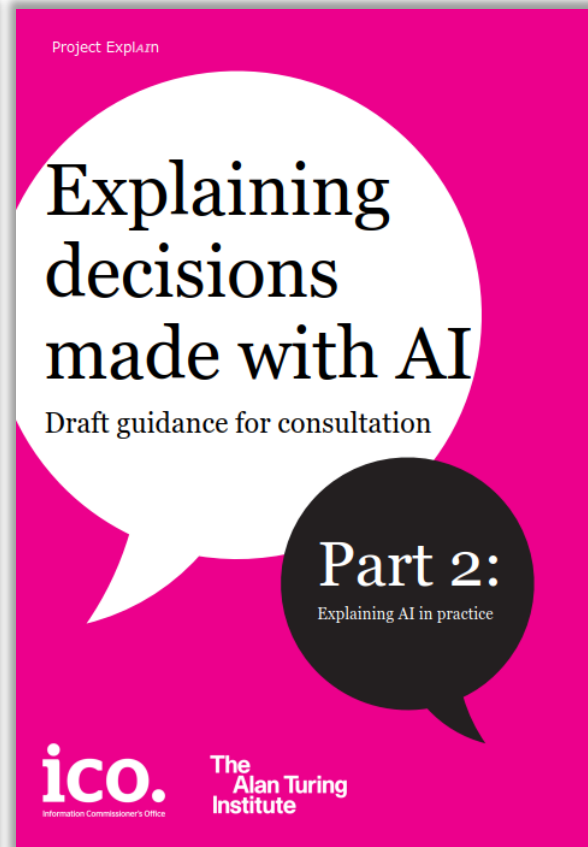
Guidance on the AI auditing framework

Управление уполномоченного по делам информации Соединенного Королевства (Information Commissioner's Office) 19.02.2020 инициировало публичное обсуждение проекта руководства по основам аудита ИИ. Датой завершения обсуждения является 01.04.2020.

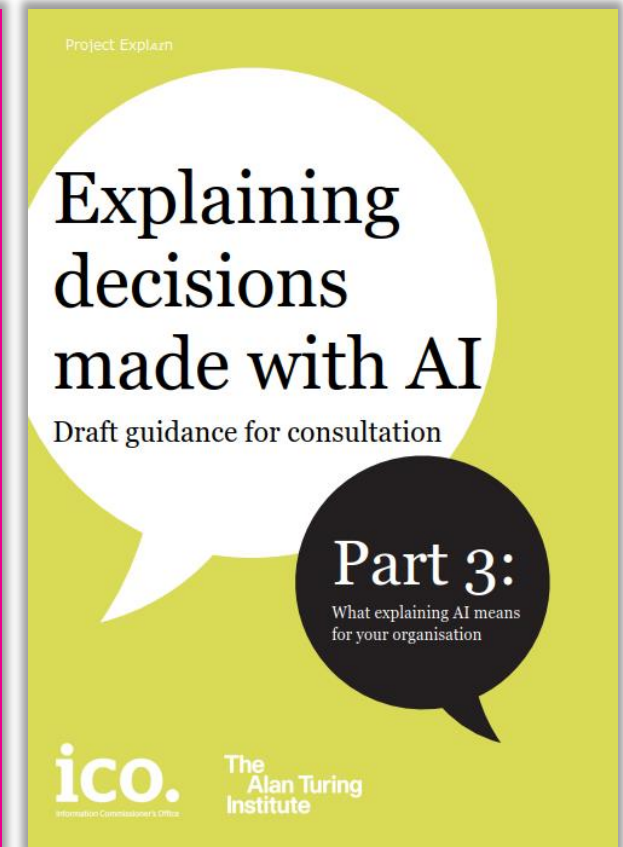
Руководство содержит рекомендации о том, как понимать закон о защите данных в отношении регулирования технологий ИИ, и рекомендации по организационным и техническим мерам по снижению рисков, которые ИИ представляет для отдельных лиц. Документ также предоставляет надежную методологию для аудита систем ИИ и обеспечения ими справедливой и законной обработки персональных данных.



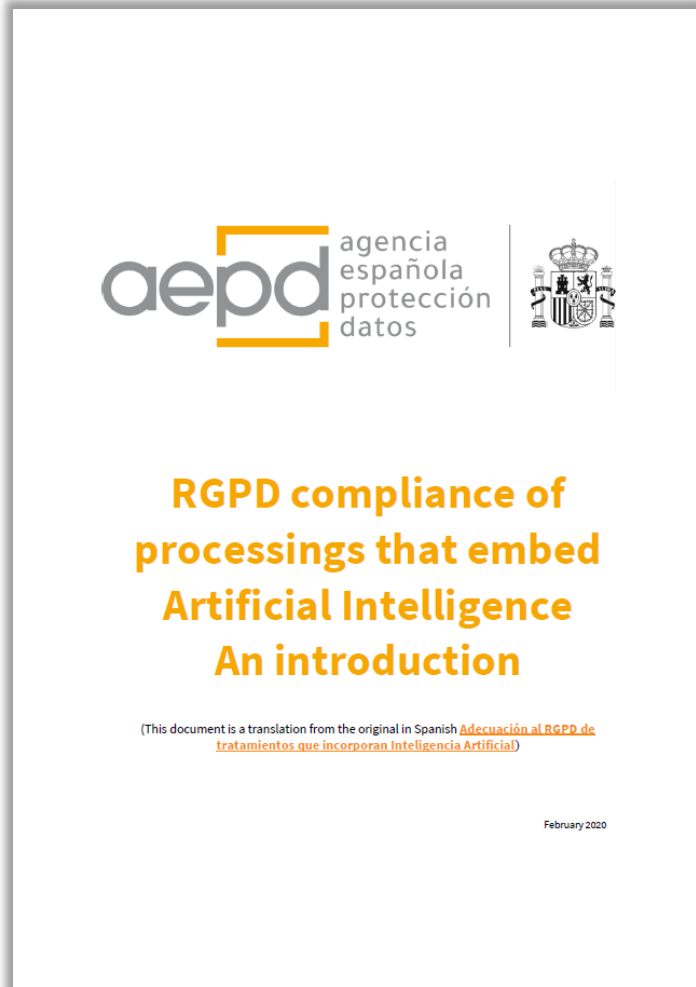
Part 1: The basics of explaining AI



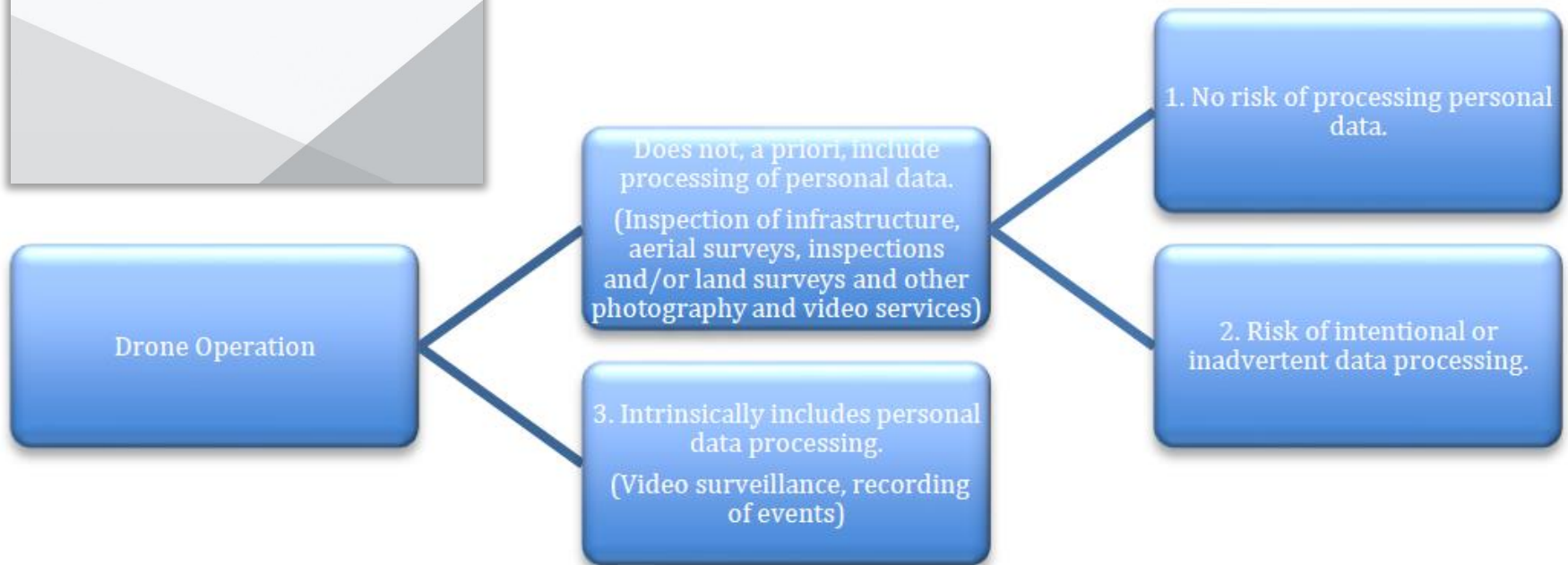
Part 2: Explaining AI in practice



Part 3: What explaining AI means for your organisation



- 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



European Commission

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 fast-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://europa.eu/!VV67my>

Publications Office of the European Union

© European Union, 2020
 Print: ISBN 978-92-76-21593-6, doi:10.2777/45473, KI-02-20-675-EN-C
 PDF: ISBN 978-92-76-21594-3, doi:10.2777/83984, KI-02-20-675-EN-H

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):





International Conference of Data
Protection & Privacy Commissioners

DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE

40th International Conference of Data Protection and Privacy Commissioners

Tuesday 23rd 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).

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.



Strasbourg, 25 January 2019

T-PD(2018)09Rev

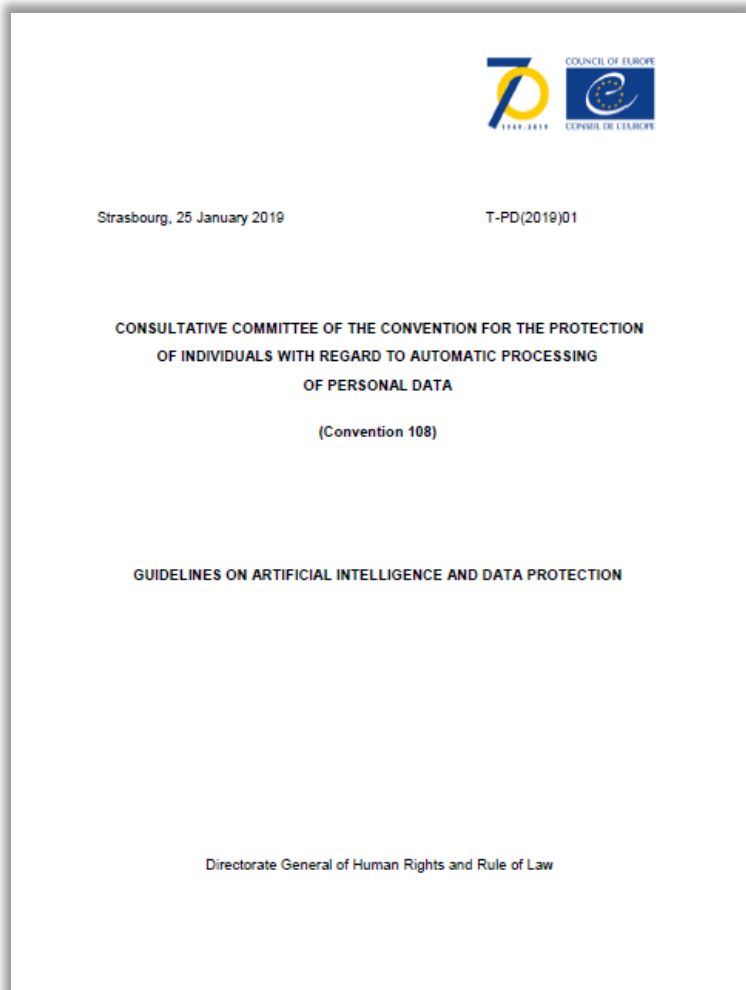
CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION
OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING
OF PERSONAL DATA

(Convention 108)

Report on Artificial Intelligence

Artificial Intelligence and Data Protection: Challenges and Possible Remedies

Directorate General of Human Rights and Rule of Law



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.

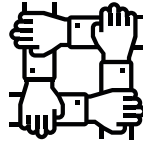
Руководство не похоже на «Три закона робототехники» Исаака Азимова. Оно не предлагает быстрых, моральных рамок, которые помогут контролировать потенциально опасных роботов. Вместо этого Руководство анализирует различные этические аспекты использования ИИ, которые будут влиять на общество, поскольку все 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.



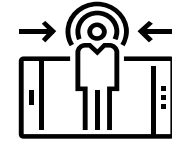
Lawful

Respecting all applicable laws and regulations



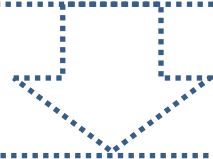
Ethical

Respecting ethical principles and values



Robust

Both from a technical perspective while taking into account its social environment



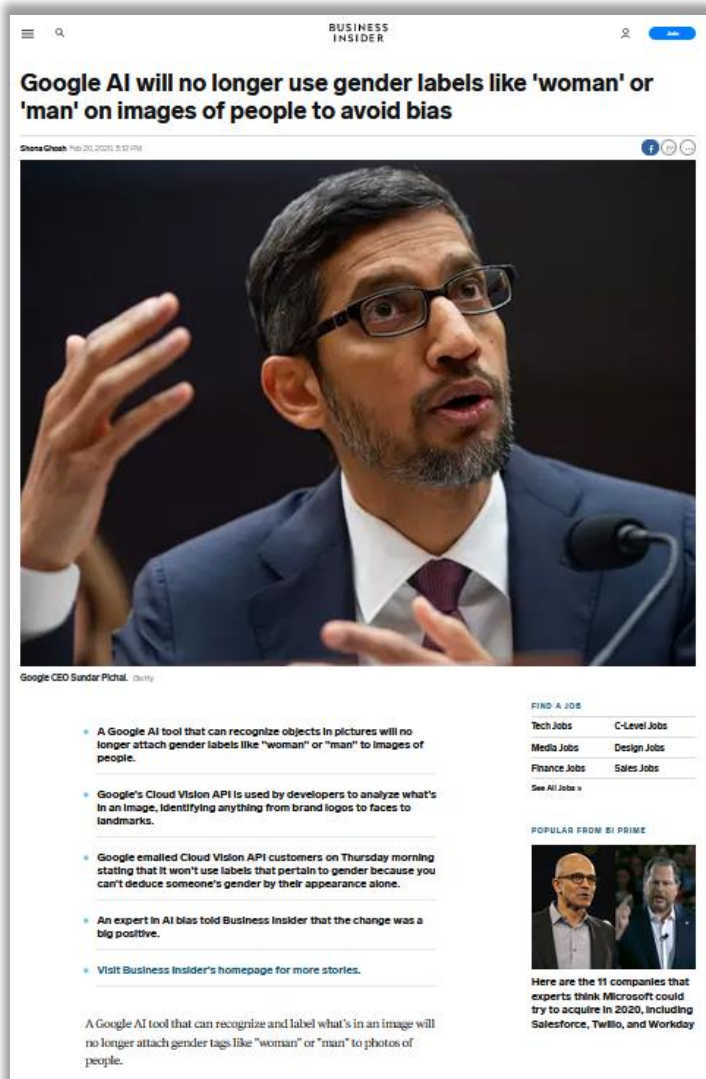
- ✓ Human agency and oversight
- ✓ Technical robustness and safety
- ✓ Privacy and Data governance
- ✓ Transparency
- ✓ Diversity, non-discrimination and fairness
- ✓ Societal and environmental well-being
- ✓ Accountability



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.

number of mentions	Principles on AI	Emerging Ethics for Artificial Intelligence	Artificial Intelligence at Google	OpenAI Ethics & Safety Principles	Microsoft AI Principles	IT AI Safety Principles	Ethically Aligned Design: A Vision for Making Human-Centered and Value-Based AI Systems (First Edition)	Ethically Aligned Design: A Vision for Making Human-Centered and Value-Based AI Systems (Second Edition)	OpenAI Charter	Assessment Report for the European Commission of Artificial Intelligence	Principles for Accessible Algorithms and a Social Impact Statement for Algorithms	AI Now 2019 Report	AI Now 2018 Report	AI Now 2017 Report	AI Now 2016 Report	The Address: AI Principles	Artificial Intelligence	The Malicious Use of Artificial Intelligence	OECD Recommendation of the Council on Artificial Intelligence	Beijing AI Principles	Report on the Future of Artificial Intelligence	The European Commission's Artificial Intelligence Strategy	
authors	(Partnership on AI 2018)	(Culier et al. 2018)	(Google 2018)	(DeepMind)	(Microsoft Corporation 2019)	(Information Technology Council 2017)	(The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems 2016)	(The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems 2019)	(OpenAI 2016)	(Abene et al. 2018)	(Dakopoulos et al.)	(Crowford et al. 2019)	(Whittaker et al. 2018)	(Carpelo et al. 2017)	(Crowford et al. 2016)	(Future of Life Institute 2017)	(Floridi et al. 2018)	(Brundage et al. 2018)	(Organisation for Economic Co-operation and Development 1 2019)	(Beijing Academy of Artificial Intelligence 2019)	(Holdren et al. 2016)	(Niska et al. 2018)	
key issue	principles of an association between several industry leaders	IBM's short list of keywords for the ethical use of AI	several short principles for the ethical use of AI	several short principles for the ethical use of AI	several short principles for the ethical use of AI	several short principles for the ethical use 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	code of ethics released by the Universitat de Montserrat	principles of the FAT ML community	statements on social implications of AI	statements on social implications of AI	statements on social implications of AI	statements on social implications of AI	large collection of different principles	meta-analysis about principles for the beneficial use of AI	analysis of abuse scenarios of AI	AI principles of the OECD	AI principles of China	AI principles of the US	AI principles of the EU	
privacy protection																							
fairness, non-discrimination, justice																							
accountability																							
transparency, openness																							
safety, cybersecurity																							
common good, sustainability, wellbeing																							
human oversight, control, auditing																							
solidarity, inclusion, social cohesion																							
explainability, interpretability																							
science-policy link																							
legislative framework, legal status of AI systems																							
future of employment/worker rights																							
responsibility/intellectual research funding																							
public awareness, education about AI and its risks																							
disinformation, military, AI arms race																							
field-specific deliberations (health, military, mobility etc.)																							
human autonomy																							
diversity in the field of AI																							
certification for AI products																							
protection of whistleblowers																							
cultural differences in the ethically aligned design of AI systems																							
hidden costs (labeling, clickwork, content moderation, energy, resources)																							
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	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	ns	ns
length (number of words)	16946	22787	756	3249	34017	8609	646	12530	16273	23759	38970	12970	4754	441	40915	108092	2272	75	417	892	4488	1481	
affiliation (government, industry, science)	government	government	science/gov./ind.	government	science	science	science	science	science	science	science	science	science	science	science	science	science	science	science	science	science	science	science
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	6	8



Google AI will no longer use gender labels like 'woman' or 'man' on images of people to avoid bias

Shana Ghosh Feb 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».

Автоматизация Privacy и Data Protection





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 :~$
```

CNIL.

To protect personal data, support innovation, preserve individual liberties

DATA PROTECTION | TOPICS | THE CNIL |  

The open source PIA software helps to carry out data protection impact assesment

12 December 2018

The PIA software aims to help data controllers build and demonstrate compliance to the GDPR. The tools is available in French and in English. It facilitates carrying out a data protection impact assessment, which will become mandatory for some processing operations as of 25 May 2018. This tool also intends to ease the use of the PIA guides published by the CNIL.

Pia | analyse d'impact sur la protection des données
privacy impact assesment

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.



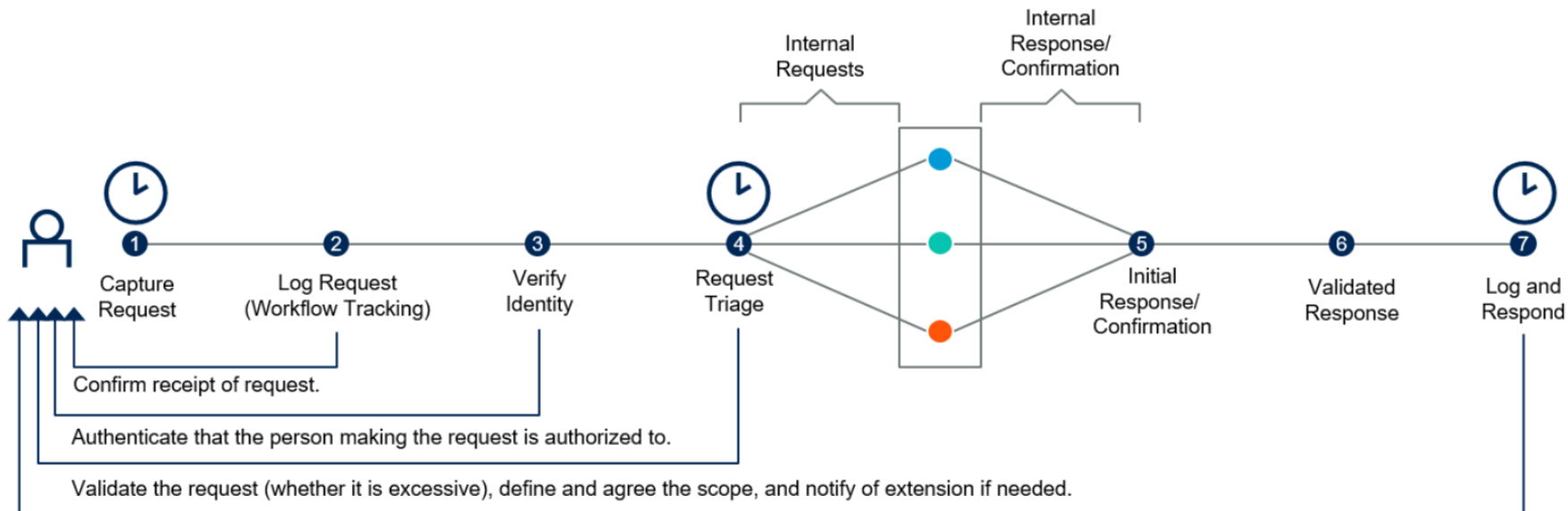
THE FORRESTER WAVE™ Privacy Management Software

Q1 2020

Market presence



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

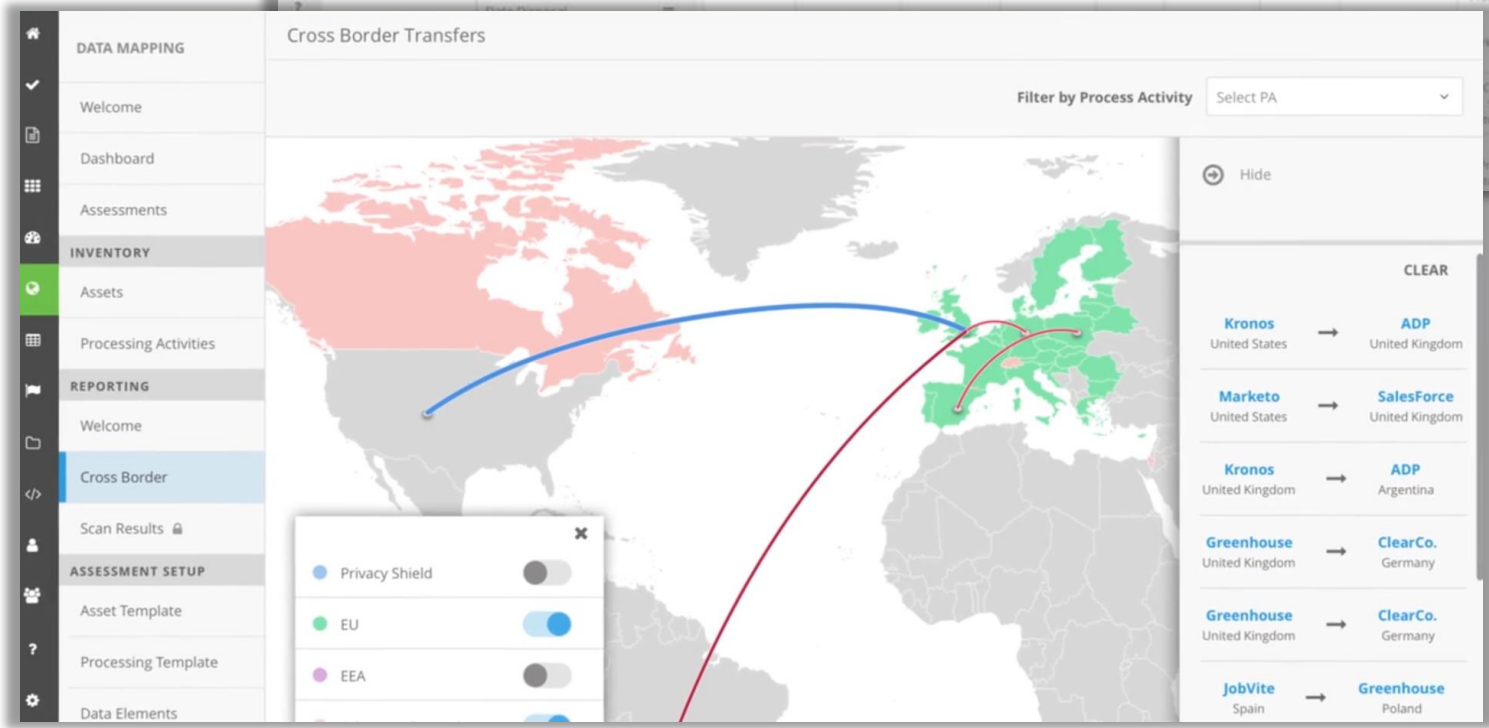
GDPR & Global Privacy Solutions

-  GDPR Validation Program
-  GDPR Compliance
-  California Consumer Privacy Act
-  Brazil Law Compliance

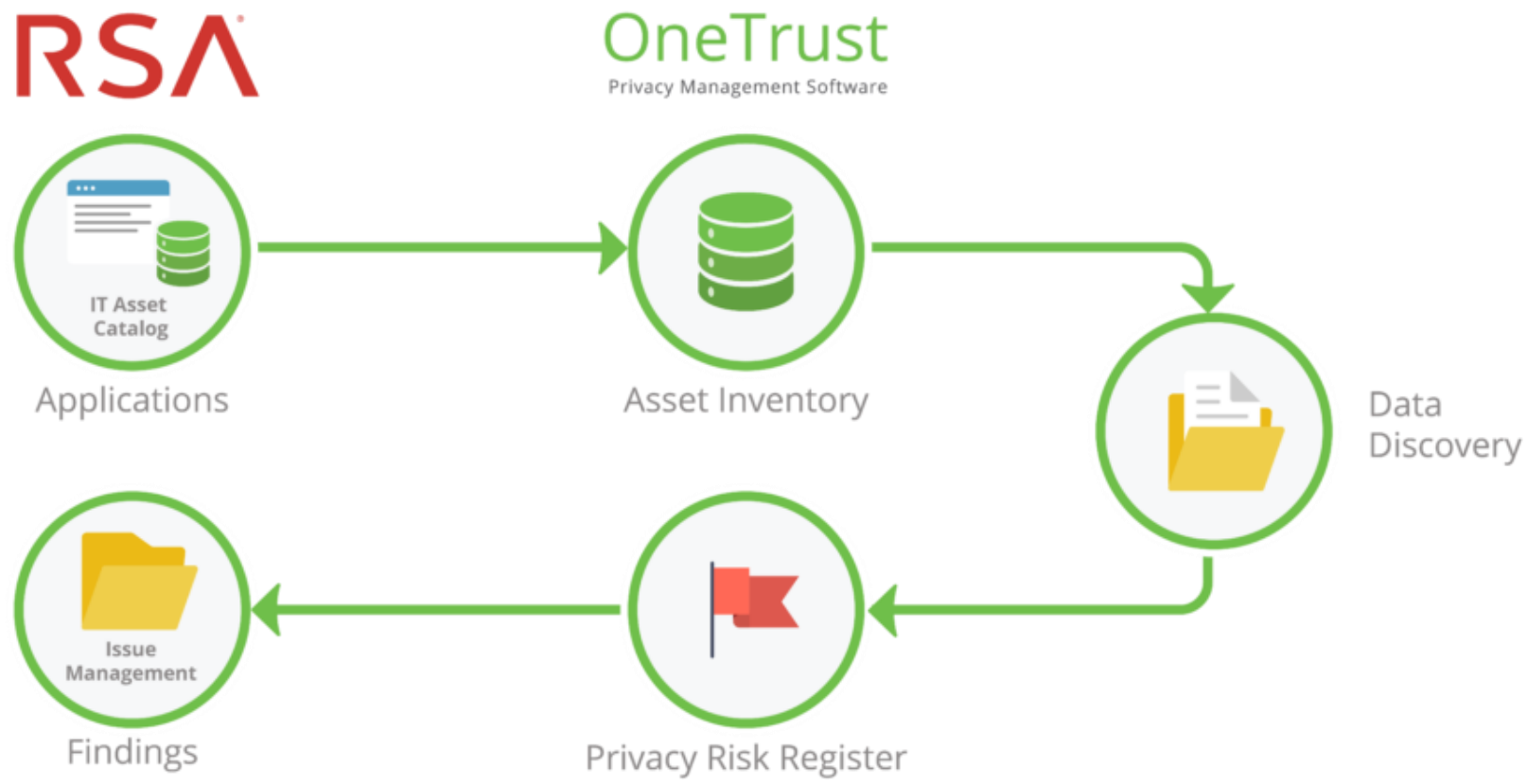
Reports / GDPR Article 30 Basic Requirements

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







ARIS Business Architect

File Edit View Insert Format Compare Arrange Hide/Show Evaluate Window Help

Balanced Scorecard

Modules Designer

Navigation Explorer tree Objects Model overview

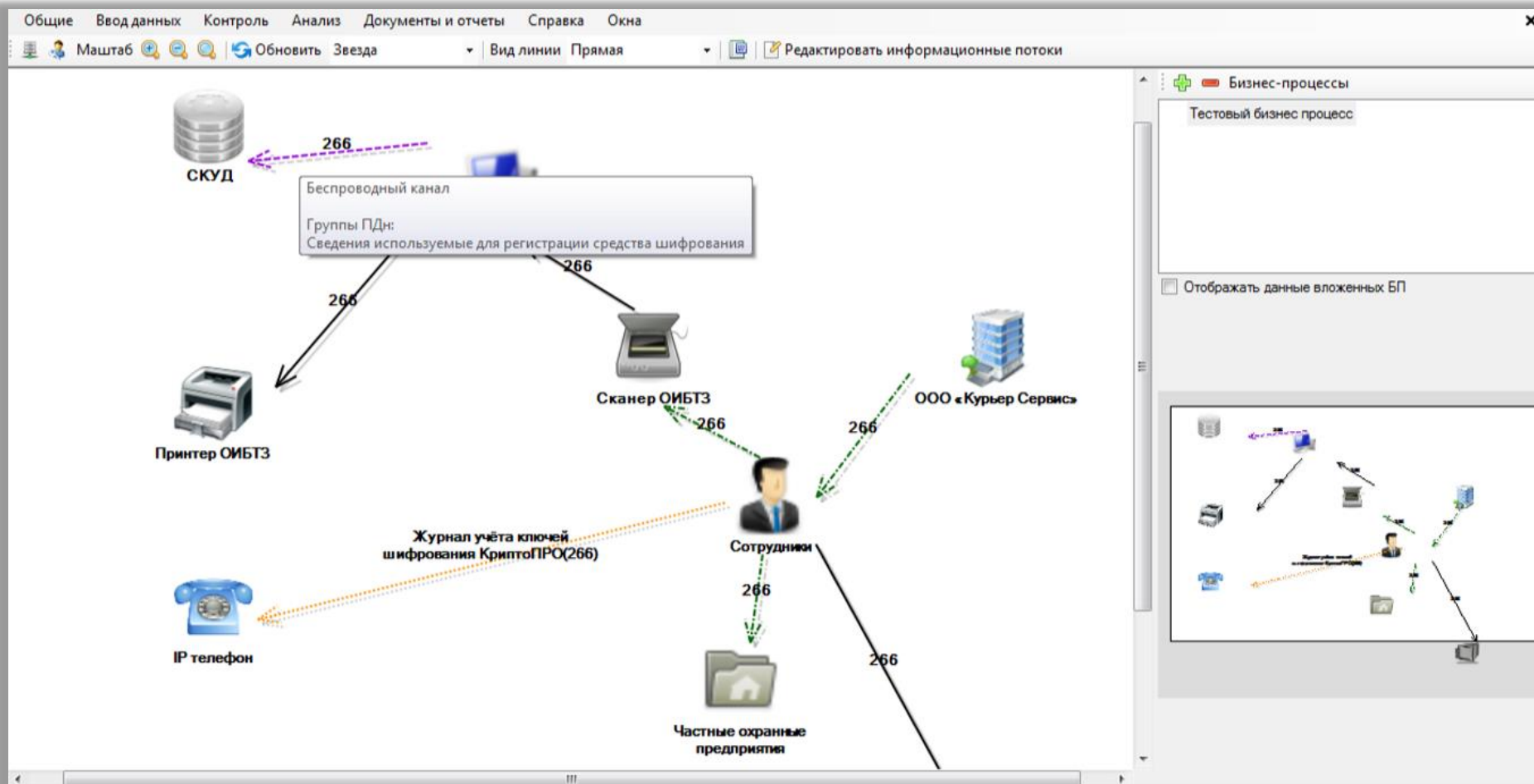
Properties Attributes Connected objects

Attribut...	Balanced	Untitled
Name	Balanced Scorecard	
Identifier		
Descript...		
Synonyms		
Full name		
Remark/...		
Time of ...	2010-2-...	2010-2-...
Creator	system	system
Author	Методи	

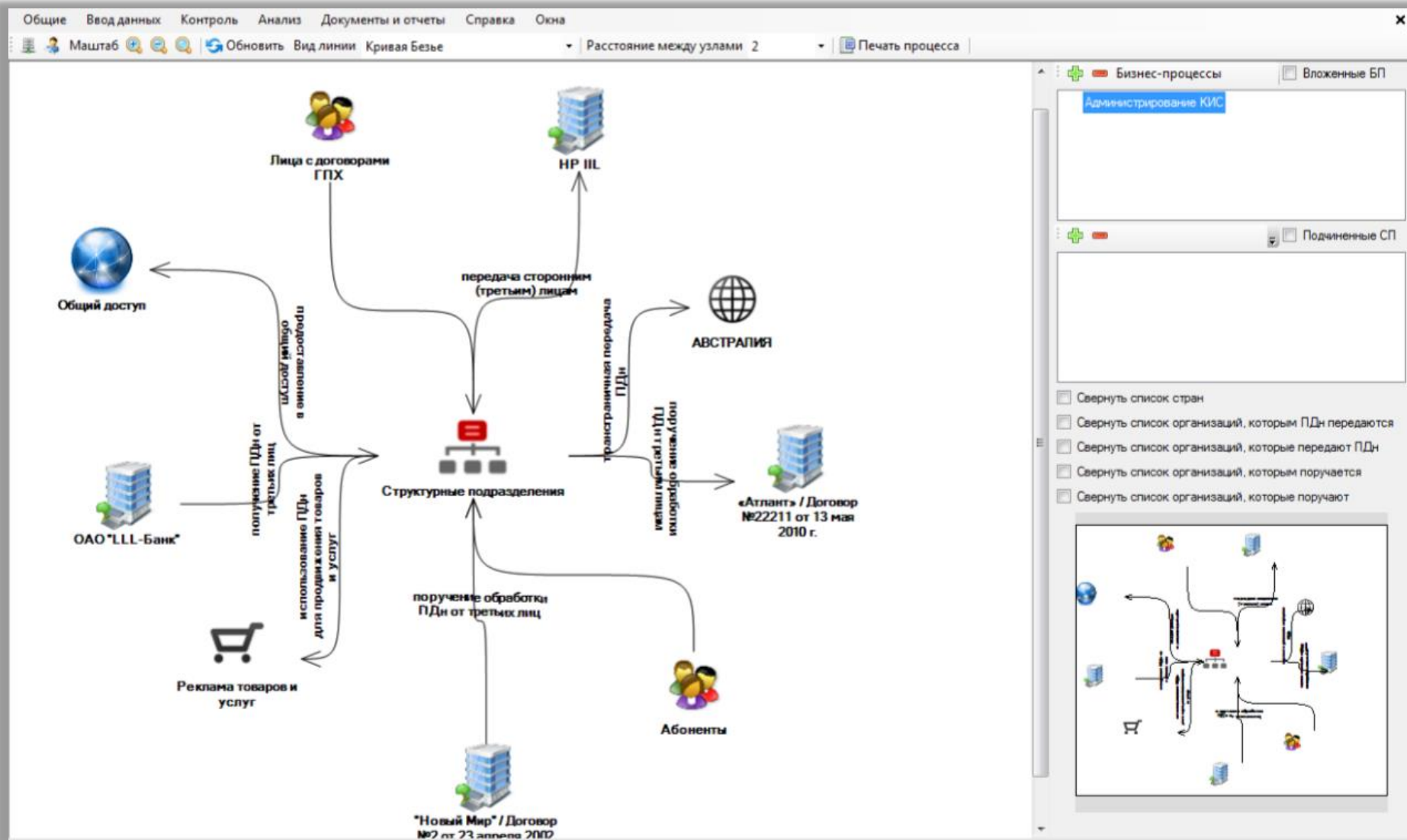
More attributes...

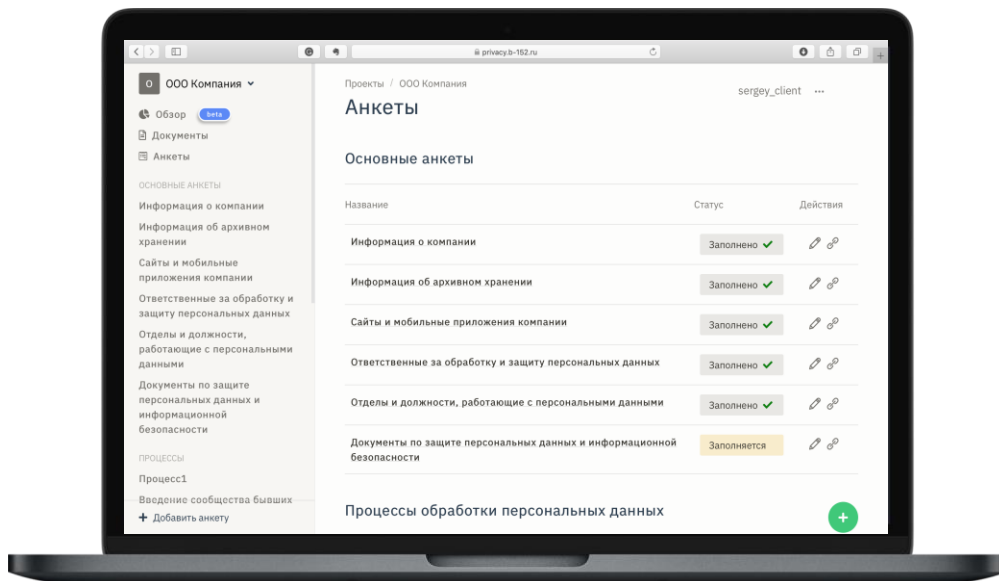
Balanced Scorecard

Rel. per...	Cause-and-effect	Cause-and-effect
Strategy	Cause-and-effect diagram with icons and text.	
Perspective	Cause-and-effect diagram with icons and text.	
Perspective	Cause-and-effect diagram with icons and text.	
Perspective	Cause-and-effect diagram with icons and text.	
Perspective	Cause-and-effect diagram with icons and text.	



Privacy-SPS включено в Единый реестр российских программ для электронных вычислительных машин и баз данных - <https://reestr.minsvyaz.ru/reestr/73559/>



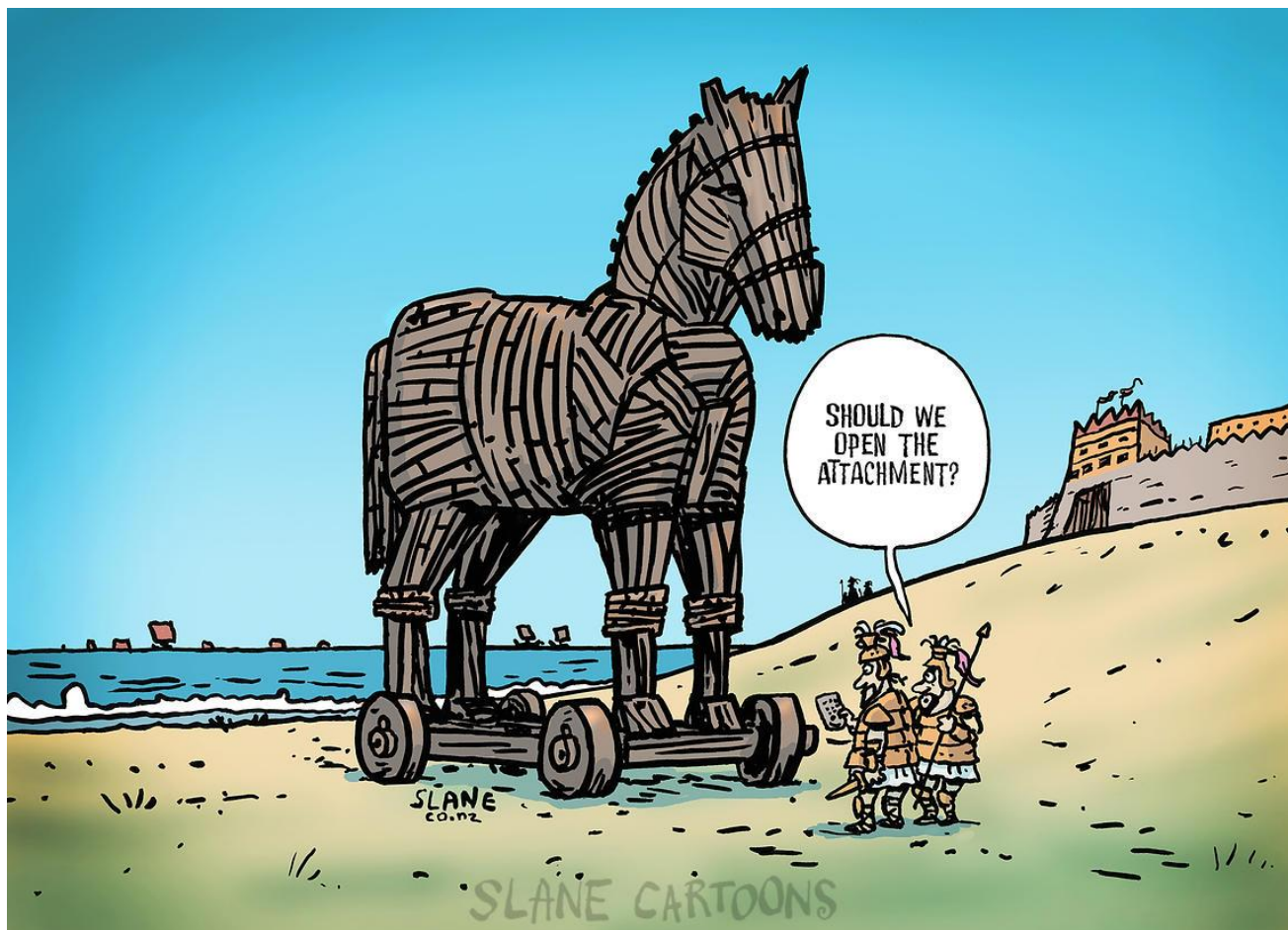


Возможности платформы:

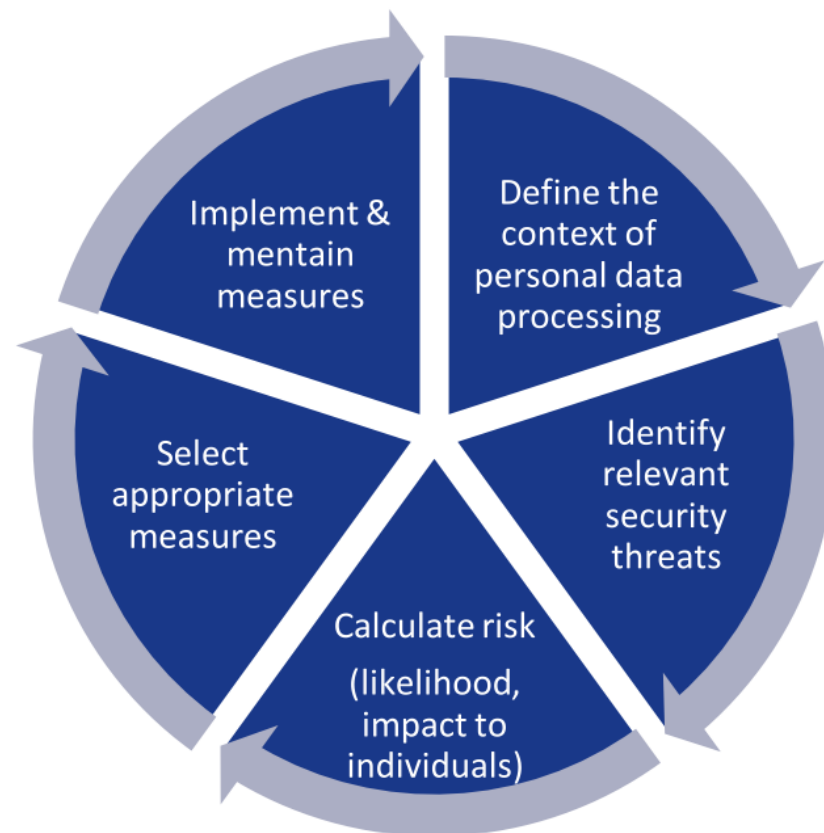
- Создание и отправка ссылок на анкеты ответственным и контроль хода их заполнения
- Использование предзаполненных анкет на основе вида деятельности компании и нашей экспертизы
- Автоматическая загрузка данных о компании из открытых источников для упрощения процесса сбора информации
- Сбор информации о сайтах с помощью искусственного интеллекта
- Выгрузка и работа с удобным протоколом со всей собранной информацией по компании

	Excel + Email	PrivacyBox
Сбор и хранение информации	✓	✓
Назначение ответственных и контроль заполнение анкет	✗	✓
Автоматическая загрузка данных о компании из открытых источников	✗	✓
Предзаполнение анкет на основе вида деятельности компании	✗	✓
Анализ сайтов с помощью искусственного интеллекта	✗	✓

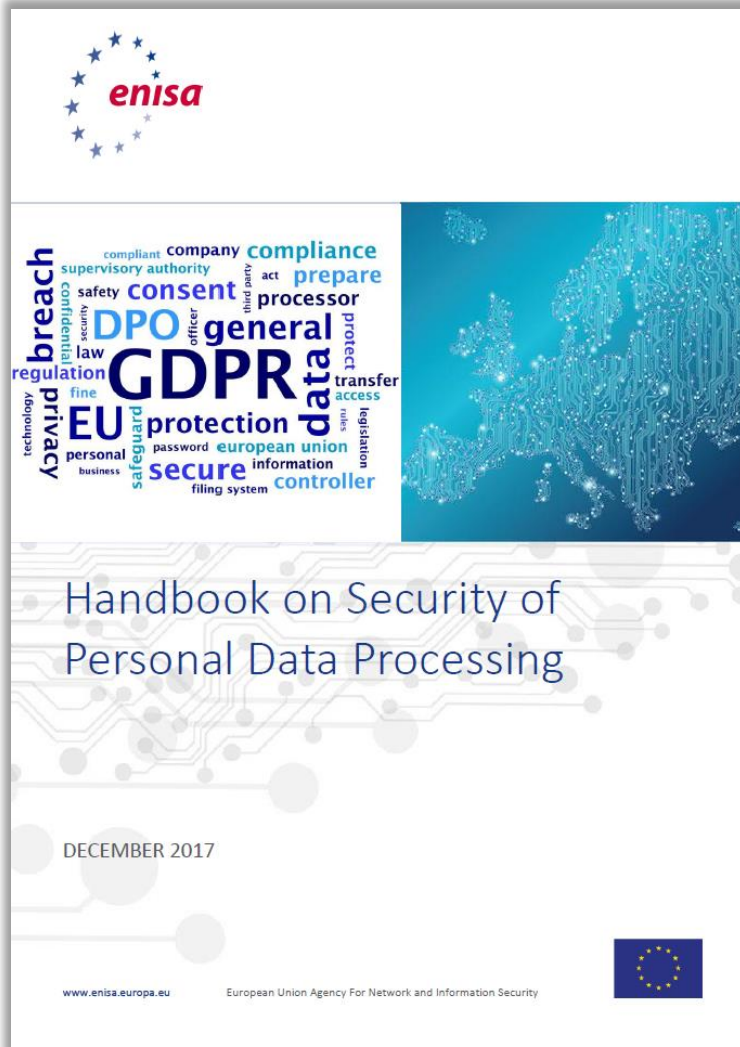
Защита персональных данных



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



ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	<input type="checkbox"/> Low	1
	<input type="checkbox"/> Medium	2
	<input type="checkbox"/> High	3
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	<input type="checkbox"/> Low	1
	<input type="checkbox"/> Medium	2
	<input type="checkbox"/> High	3
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	<input type="checkbox"/> Low	1
	<input type="checkbox"/> Medium	2
	<input type="checkbox"/> High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	<input type="checkbox"/> Low	1
	<input type="checkbox"/> Medium	2
	<input type="checkbox"/> High	3

OVERALL SUM OF THREAT OCCURRENCE PROBABILITY	THREAT OCCURRENCE PROBABILITY LEVEL
4 - 5	Low
6 - 8	Medium
9 - 12	High

THREAT OCCURRENCE PROBABILITY	IMPACT LEVEL		
	Low	Medium	High / Very High
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



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



Step 1
Definition of the processing operation and its context

Types of personal data
Categories of data subjects
Means of processing
Recipients

Step 2
Understanding and evaluation of impact

Confidentiality
Integrity
Availability

Step 3
Definition of possible threats and evaluation of their likelihood

Network and technical resources
Processes/procedures related to the data processing operation
Different parties and people involved in the data processing operation
Business sector and scale of processing

Step 4
Evaluation of risk

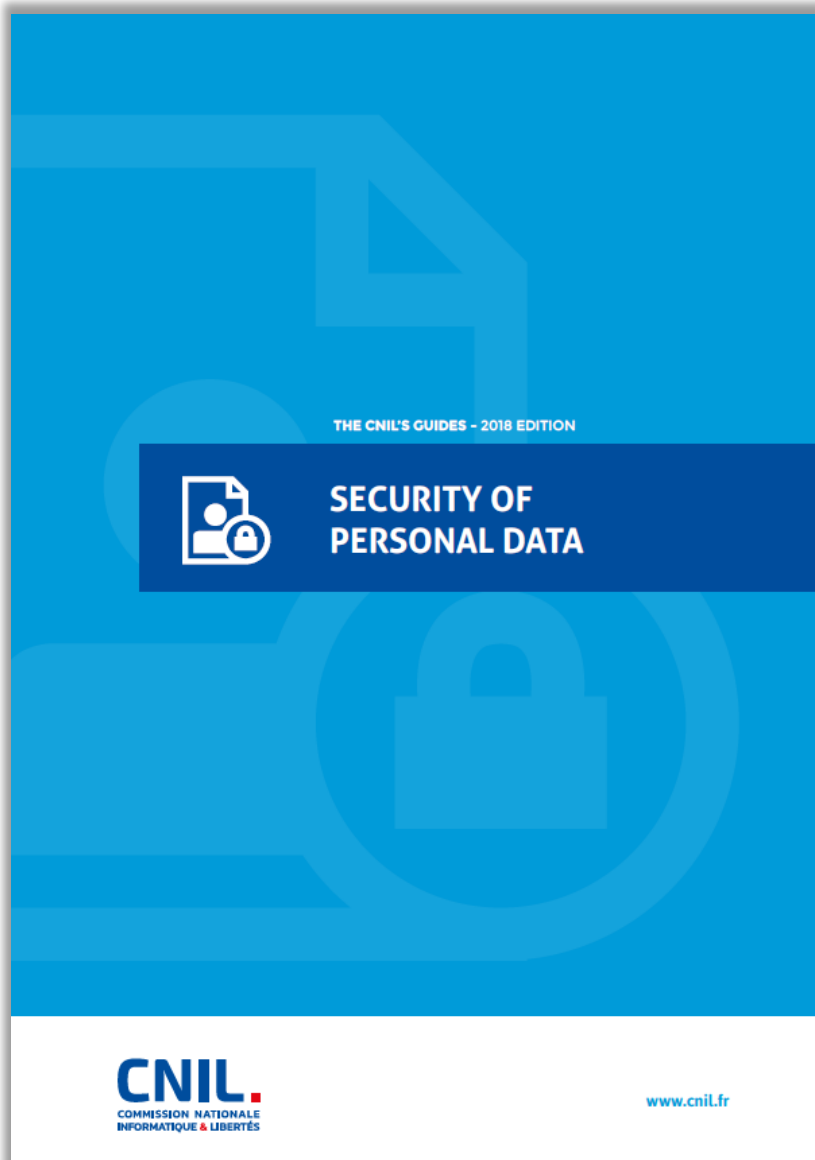
		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low			
	Medium			
	High			

Step 5
Selection of security measures

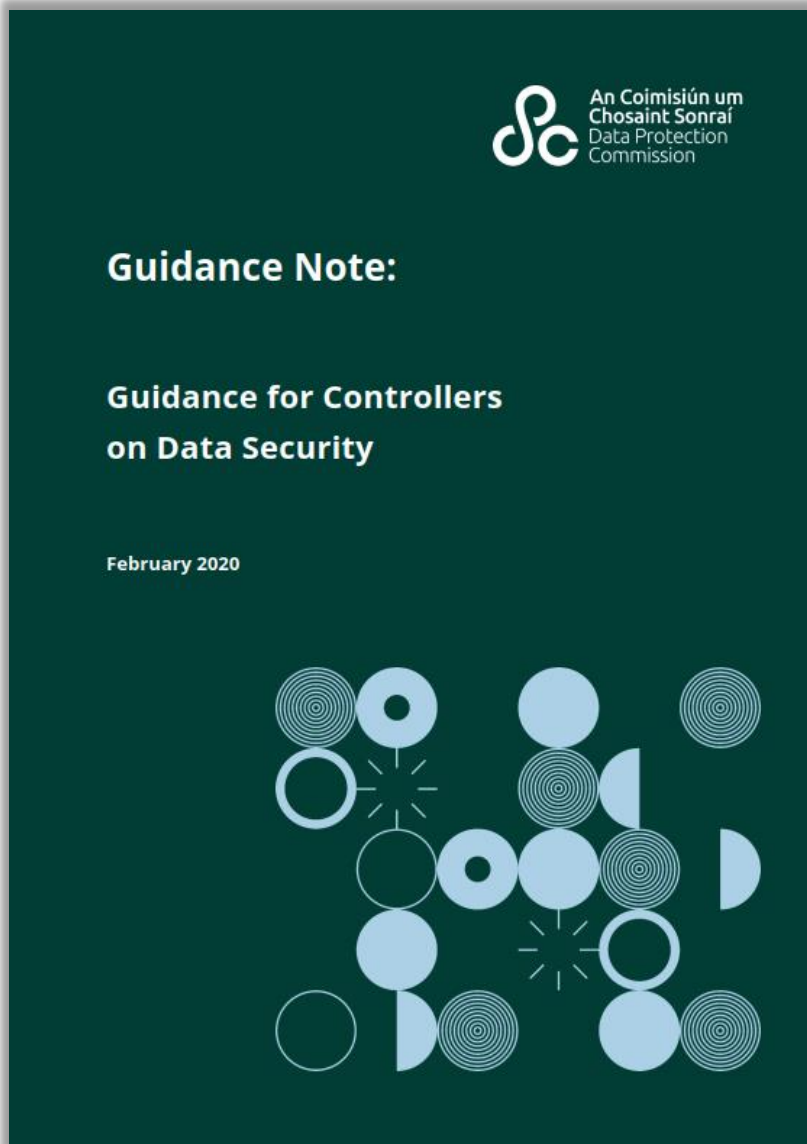


<https://www.enisa.europa.eu/risk-level-tool/>


<https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform>




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



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.....



agencia
española
protección
datos



Assessment and Technological Studies
Department
1 / 6

Recommendations to protect personal data in situations of mobility and telecommuting

The organisation, as data controller, may adopt the decision that certain activities within their company be executed in situations of mobility and telecommuting. Such a decision may be part of a management strategy, a general, or a partial strategy for certain areas or activities (for example, personnel who travels frequently) or it may be caused by exceptional or even force majeure situations.

If, in the first case, a prior planning must be carried out, in the second case, urgency situations may force the controller to put into place temporary solutions. When this occurs, it is compulsory, namely when the situation extends through time, to reflect about the situation and to perform an implementation of telecommuting in parallel. It must be taken into account that the [State's resilience](#), [the continuity of the business processes](#), and the rights and freedoms of data subjects whose data are being processed depend on it.

The organisation and the personnel that are involved in telecommuting actions must take the following recommendations into consideration.

RECOMMENDATIONS AIMED AT DATA CONTROLLERS

Below, a set of recommendations for the data controller is listed that the data controller will need to adapt to the specific situation of their business purposes:

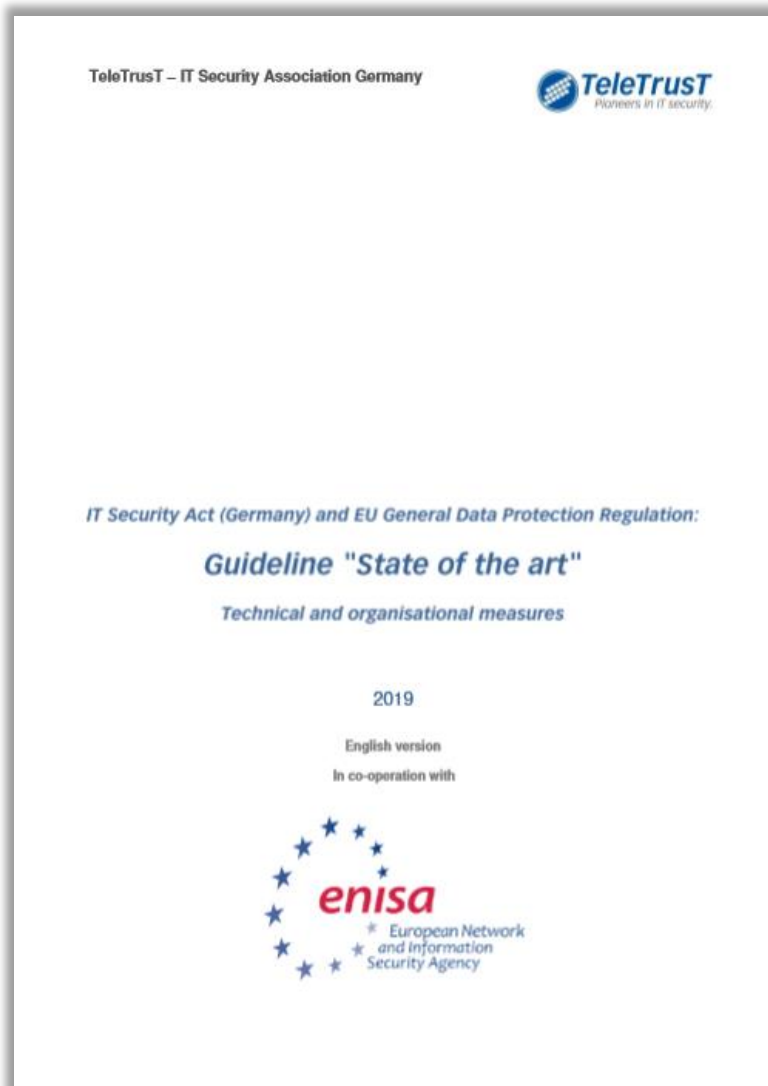
- 1. Definition of an information protection policy for mobility situations**
 - Based on the data protection policy and the Information Security of the entity, and, as part of such entity, a **specific policy for mobility situations** needs to be defined that addresses the special needs and the particular risks introduced by the access to corporate resources from spaces that are not under the control of the organisation.
 - In such policy, the determination must be made of what ways of remote access are allowed, what type of devices are valid for each way of access, and the level of access permitted pursuant to the mobility profiles defined. The responsibilities and obligations must likewise be defined to be undertaken by the persons hired.
 - It is necessary to provide functional guidelines aimed at training the persons hired, as a result of such policies, and such guidelines must include at least the information described in the section "Recommendations addressed at personnel participating in processing operations" in this document.
 - The personnel must likewise be informed of the main threats that may affect them when working outside the organisation as well as the possible consequences that may be materialised in case of breach of such directions, both for data subjects and for the employee.
 - In such guidelines, a contact person must be identified to report any incident affecting personal data, as well as the suitable channels and formats to deliver such notification.
 - The personnel must sign a telecommuting agreement that includes the undertakings acquired at the time to perform their tasks under a situation of mobility.

C/ Jorge Juan 6
28001 - Madrid

<http://www.aepd.es>
<https://sedeagpd.gob.es>

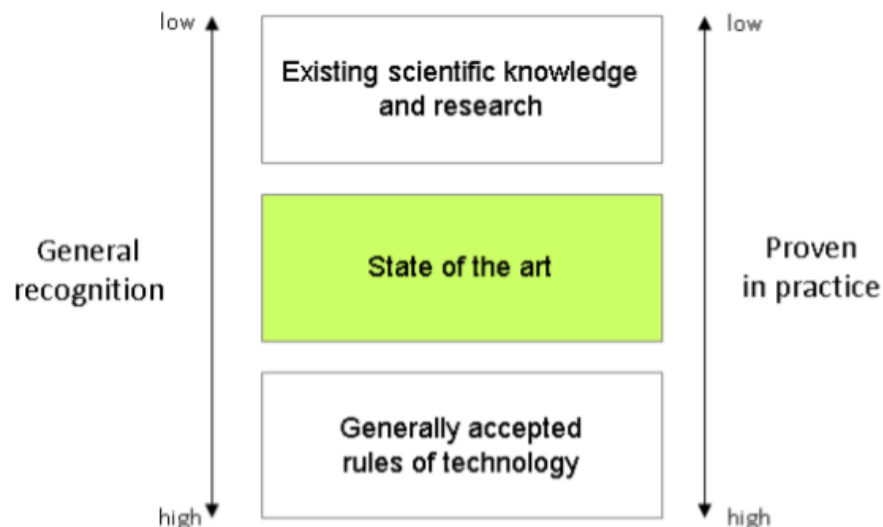
В апреле 2020 испанский уполномоченный орган опубликовал рекомендации для контролеров и их персонала по защите персональных данных в условиях мобильности и удаленного взаимодействия. В частности, рекомендуется следующее:

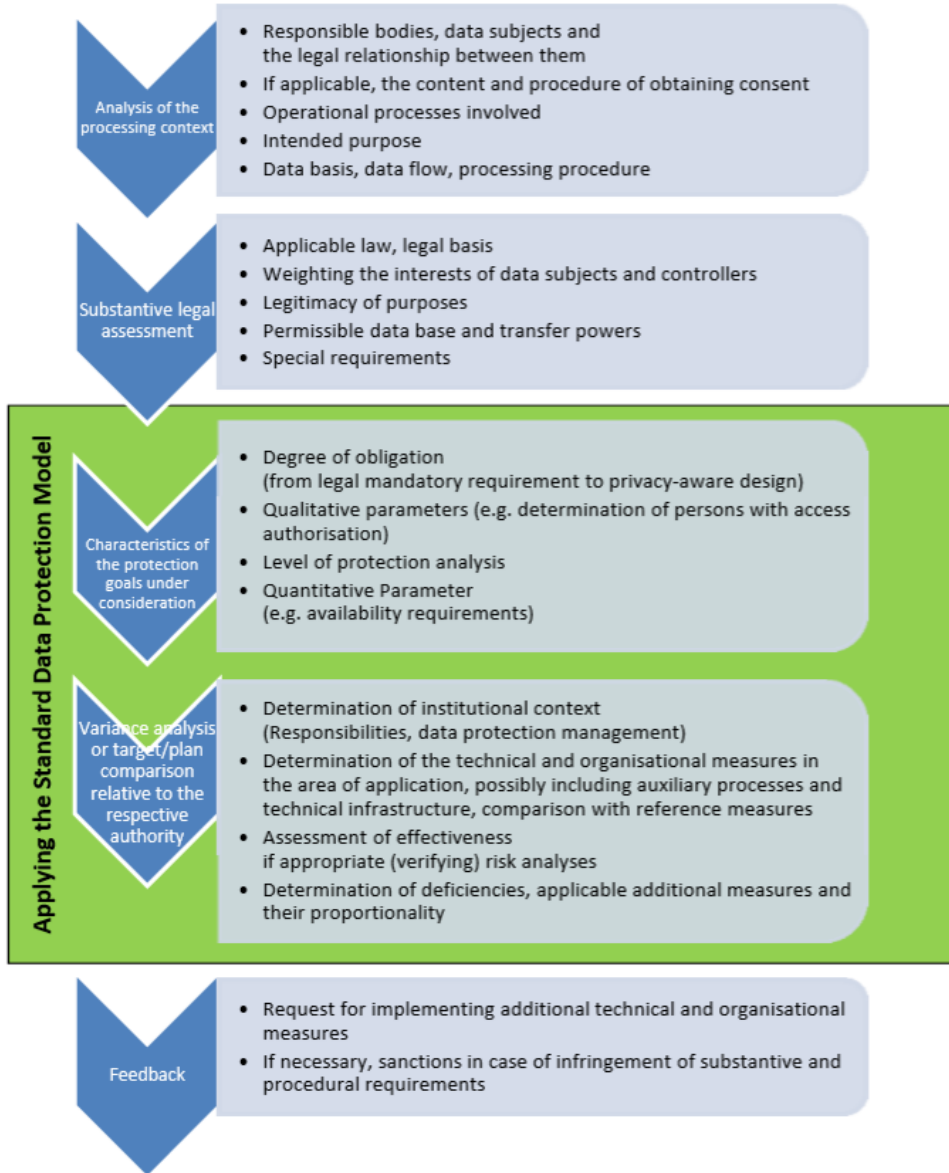
- определение политики защиты информации для условий удаленного взаимодействия;
- выбор поставщиков решений и услуг, которые заслуживают доверия и предлагают гарантии;
- ограничение доступа к информации;
- правильная настройка оборудования и устройств, используемых для удаленного взаимодействия;
- мониторинг удаленного доступа к корпоративной вычислительной сети;
- рациональное управление защитой и безопасностью данных.



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.

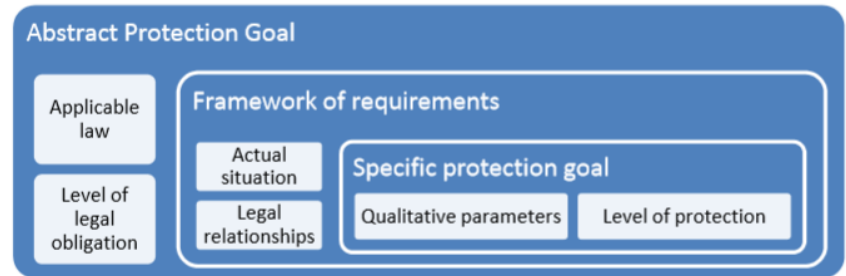




Немецкий стандарт, объединяющий в себе подходы GDPR и ИБ и являющийся концепцией аудита и консультаций на основе единых целей защиты информации.

Первая (устаревшая) версия на английском: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf

Вторая (обновлённая) версия на немецком: <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf>



EUROPEAN ARCHIVES GROUP

GUIDANCE
ON DATA PROTECTION FOR ARCHIVE SERVICES

EAG guidelines on the implementation of the General Data Protection
Regulation in the archive sector

These guidelines are intended to help archive services in Europe apply the General Data Protection Regulation. They are a work in progress, subject to improvement and enrichment, thanks to your experience and comments. These guidelines may also be amended on the basis of future jurisprudence and of opinions and guidelines issued by the European Data Protection Board.

The European Archives Group warmly welcomes your comments. Comments can be sent to the following e-mail address: SG-EAG-GUIDELINES@ec.europa.eu.

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.

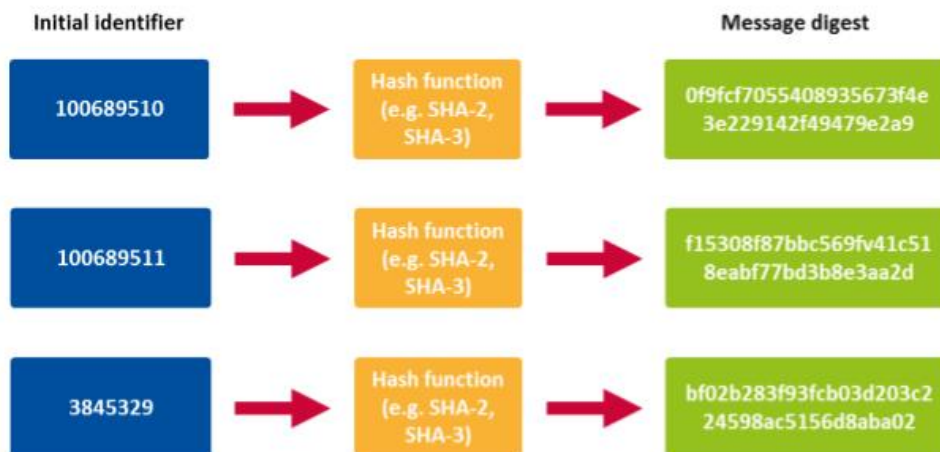
Руководство адресовано государственным и частным органам и учреждениям, в которых хранятся архивные документы (то есть те документы, которые были отобраны на постоянное хранение), включая национальные и государственные, региональные и муниципальные архивы, музеи, библиотеки, фонды и другие государственные и частные организации, сохраняющие архивные документы.



Псевдонимизация и анонимизация






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».



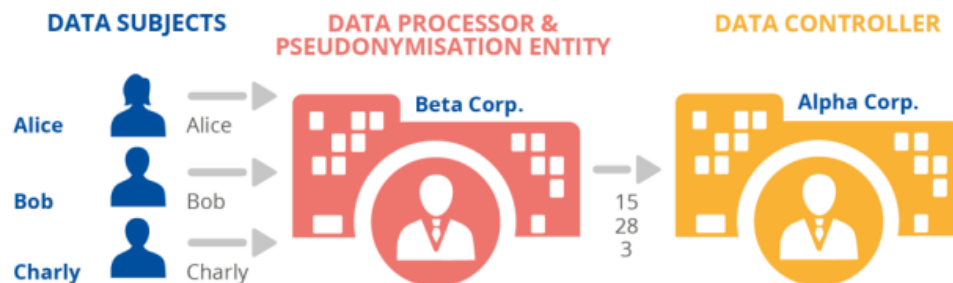
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



Pseudonymisation techniques and best practices

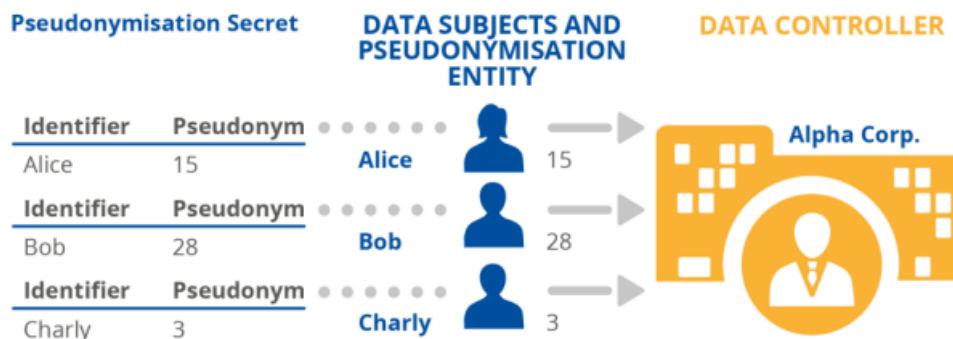
Recommendations on shaping technology according to data protection and privacy provisions

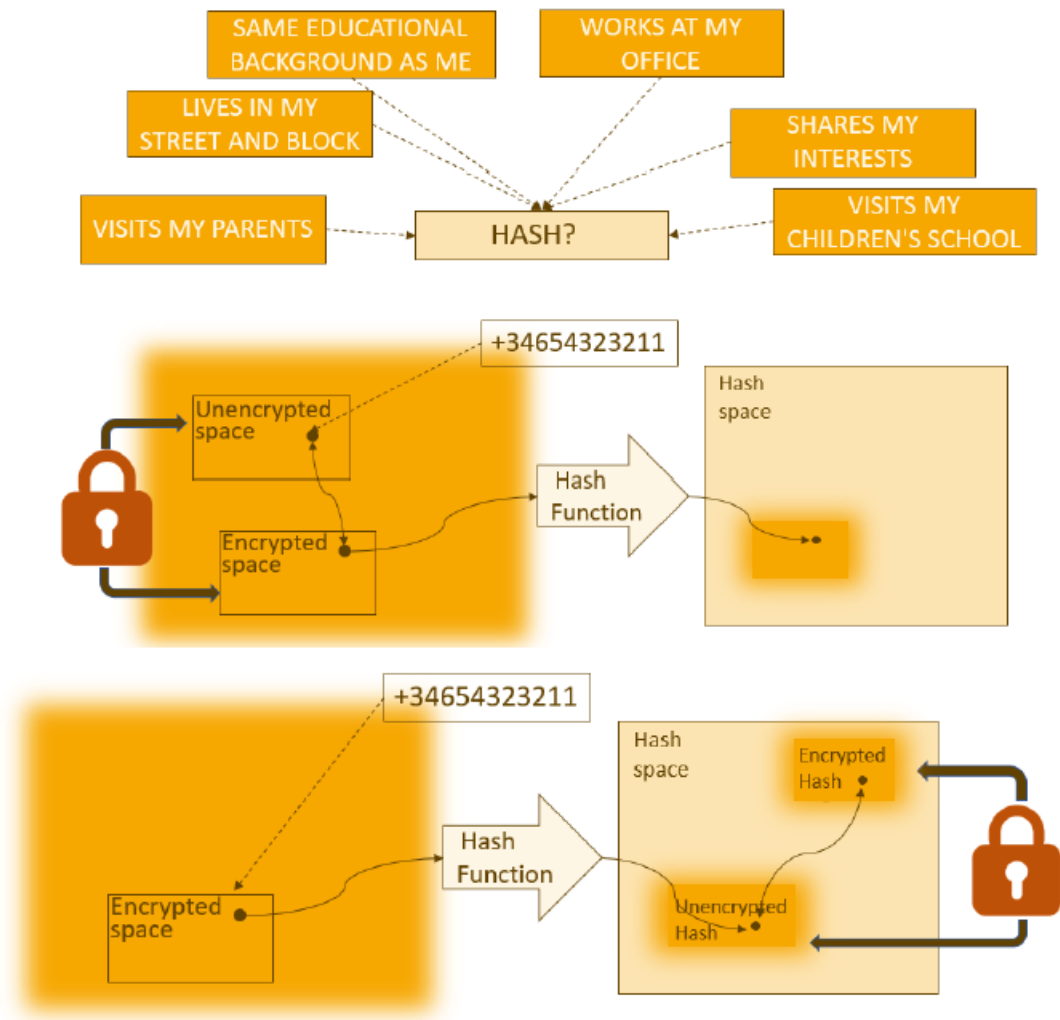
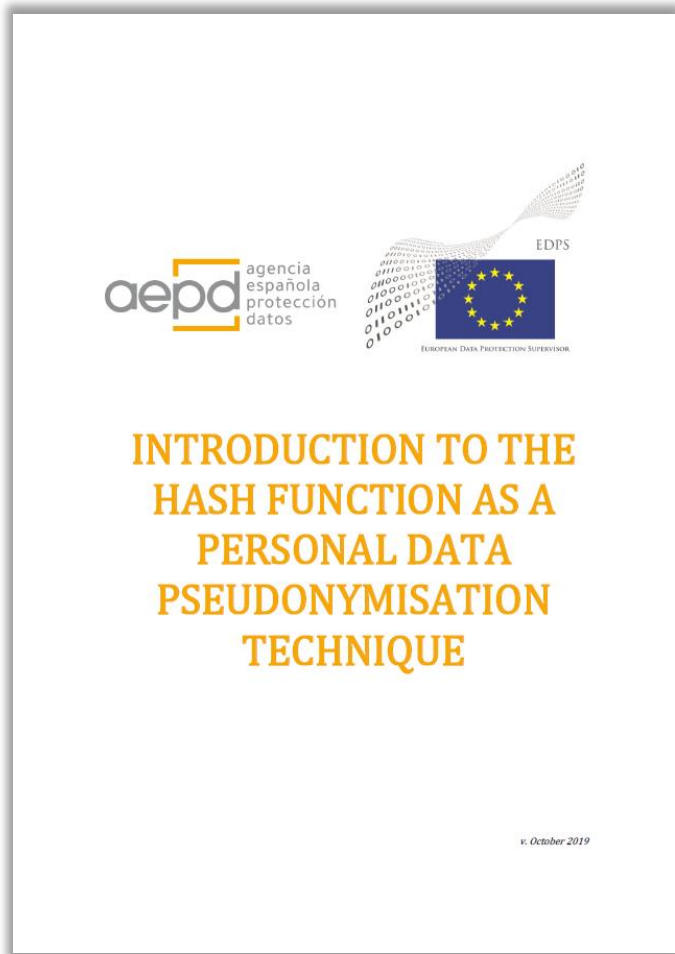
NOVEMBER 2019



Pseudonymisation Secret

Identifier	Pseudonym
Alice	15
Bob	28
Charly	3
...	...





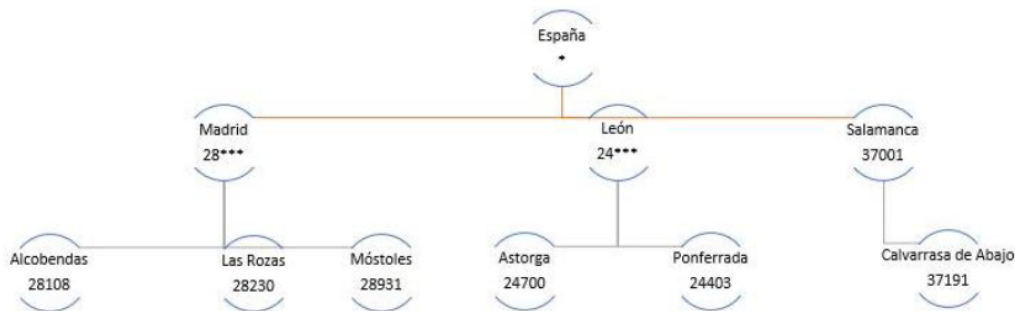
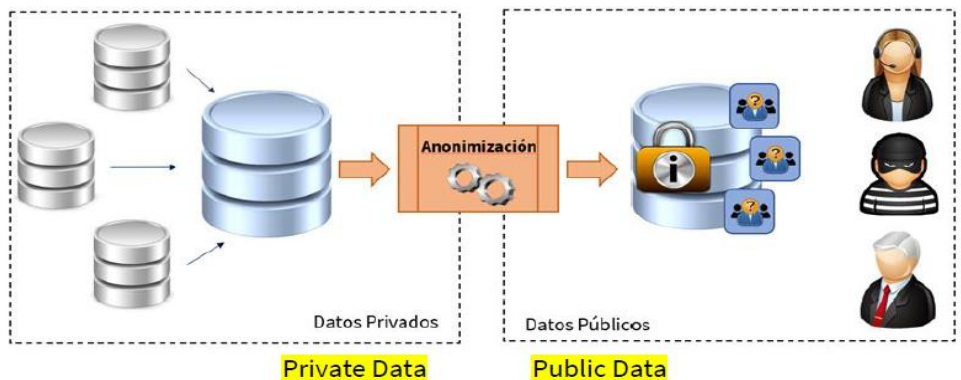


Figure 2: Hierarchy for the Postcode field

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



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.

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.

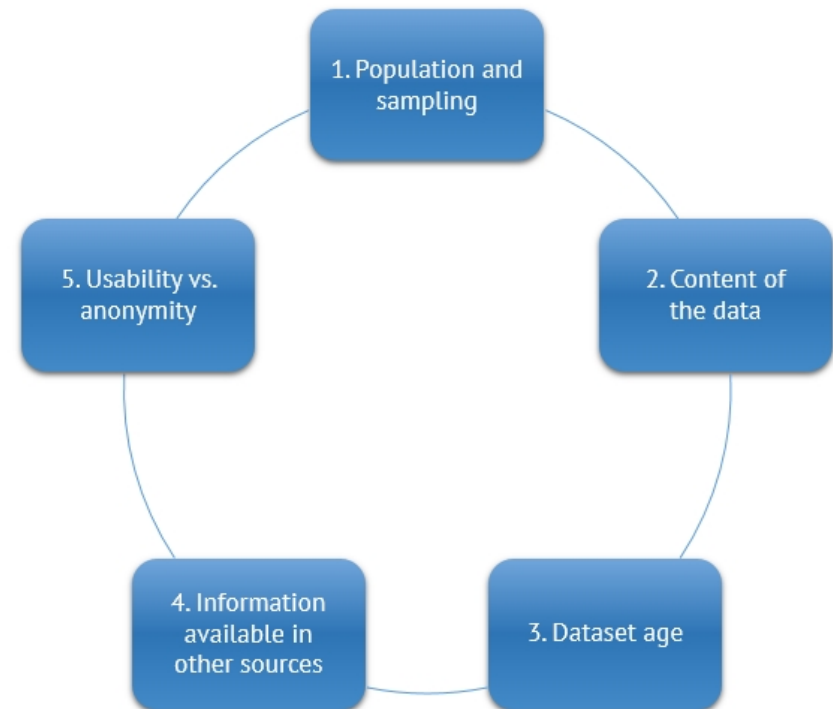
1. **Population and sampling:** *Who were the target population of the study and how was sampling conducted? How many people belonging to the population were included in the sample? What is known about the population beforehand (e.g. distribution of gender and age)? Do individuals belonging to the population 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:

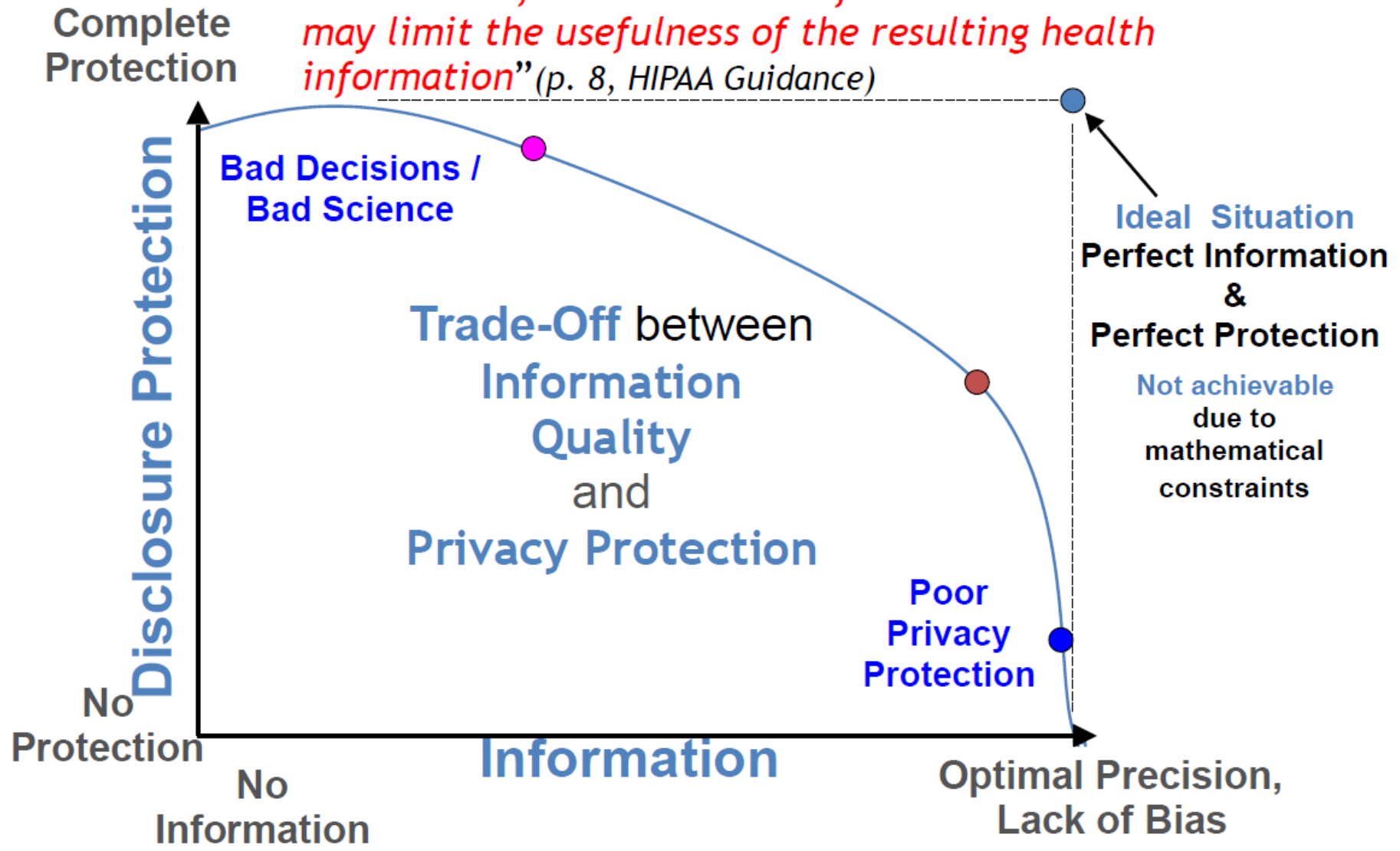
What is removed, categorised, coarsened? Quantitative datasets: How are open-ended responses processed? Note that any documents relating to anonymisation cannot contain pseudonymous information or other information based on which individuals could still be identified. For instance, lists of aliases/pseudonyms used for personal names must be destroyed when they are no longer needed.

Rationale for anonymisation and assessing disclosure risk after anonymisation:

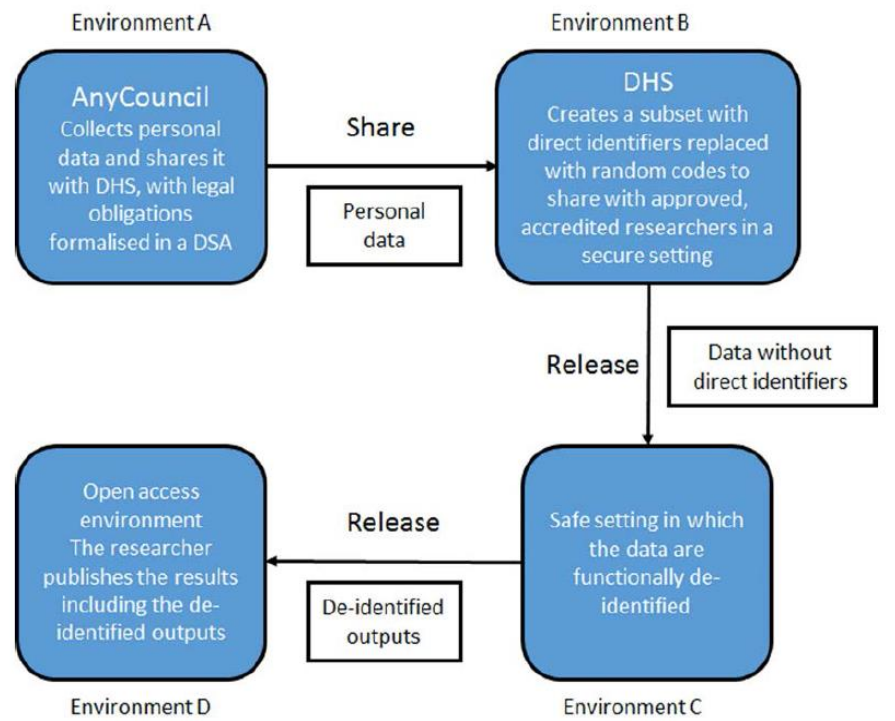
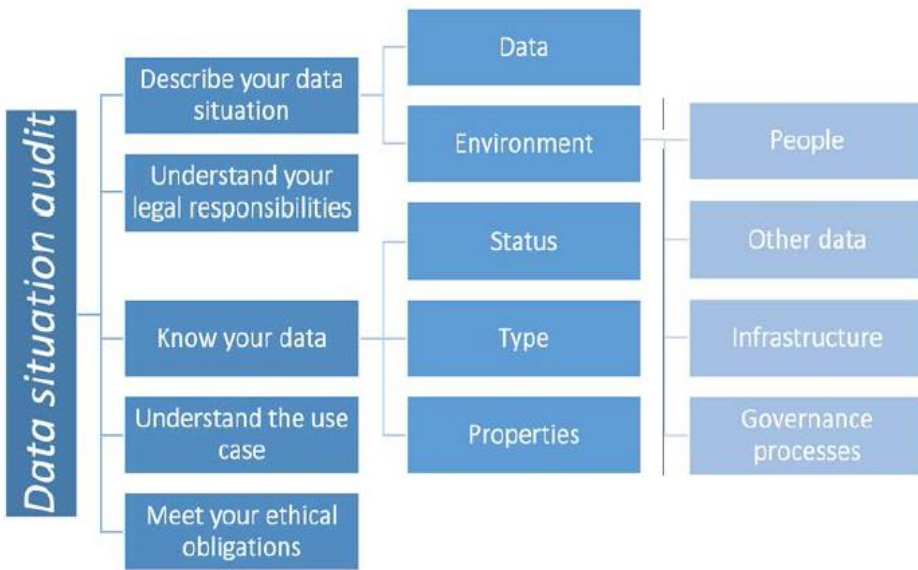
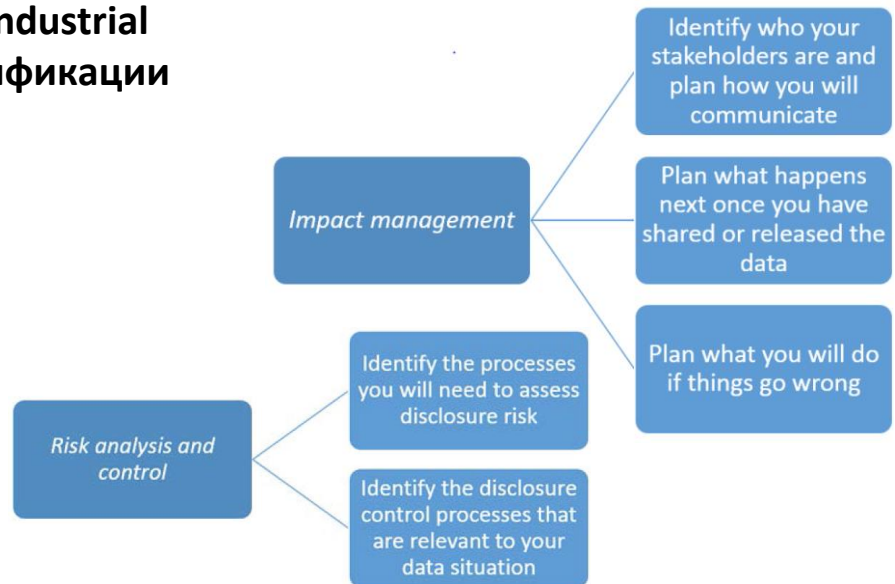
Provide rationale for anonymisation solutions and policies. Assess the possibility of identifying individuals in the data now and in the future. Think about when the anonymity of the data should be reviewed again (residual risk assessment). You can also provide further information regarding, for instance, the anonymisation process, how anonymisations are marked, and possible errors that secondary users of the data should take into account.



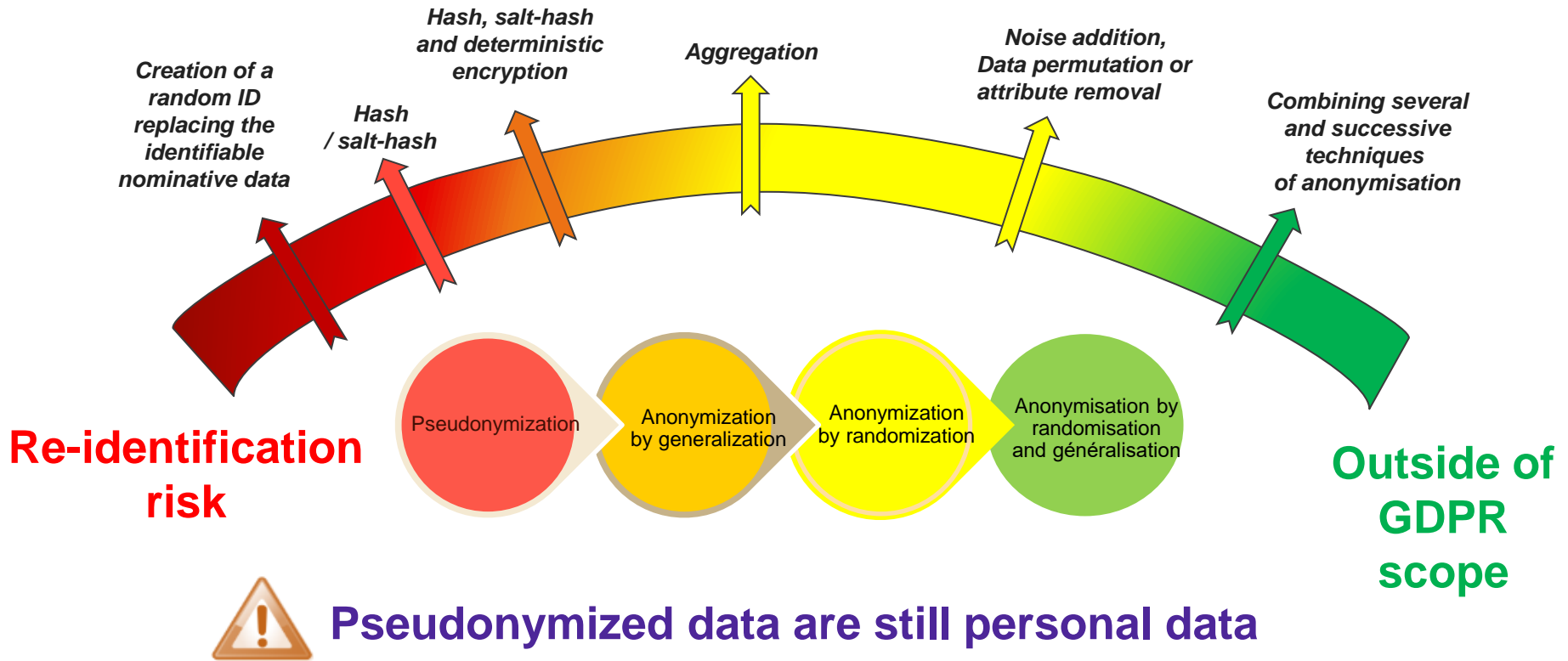
“De-identification leads to information loss which may limit the usefulness of the resulting health information” (p. 8, HIPAA Guidance)



Методология от Commonwealth Scientific and Industrial Research Organisation (Австралия) по деидентификации



WHAT IS NOT PERSONAL DATA: ANONYMISATION



Международные стандарты





[Main page](#)
[Recent changes](#)
[Wiki help](#)

▼ Organisation
 [Contacts](#)

▶ Standardisation

▶ Tools

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

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

- [CEN-CENELEC-ETSI](#)
- [IETF Activities](#)
- [IEEE standards](#)
- [ISO/IEC](#)
- [ITU standards](#)
- [OASIS](#)
- [OpenID Foundation](#)
- [W3C Activities](#)
- [National Level Standards](#)

[More info on privacy standards \[Expand\]](#)

Privacy engineering projects

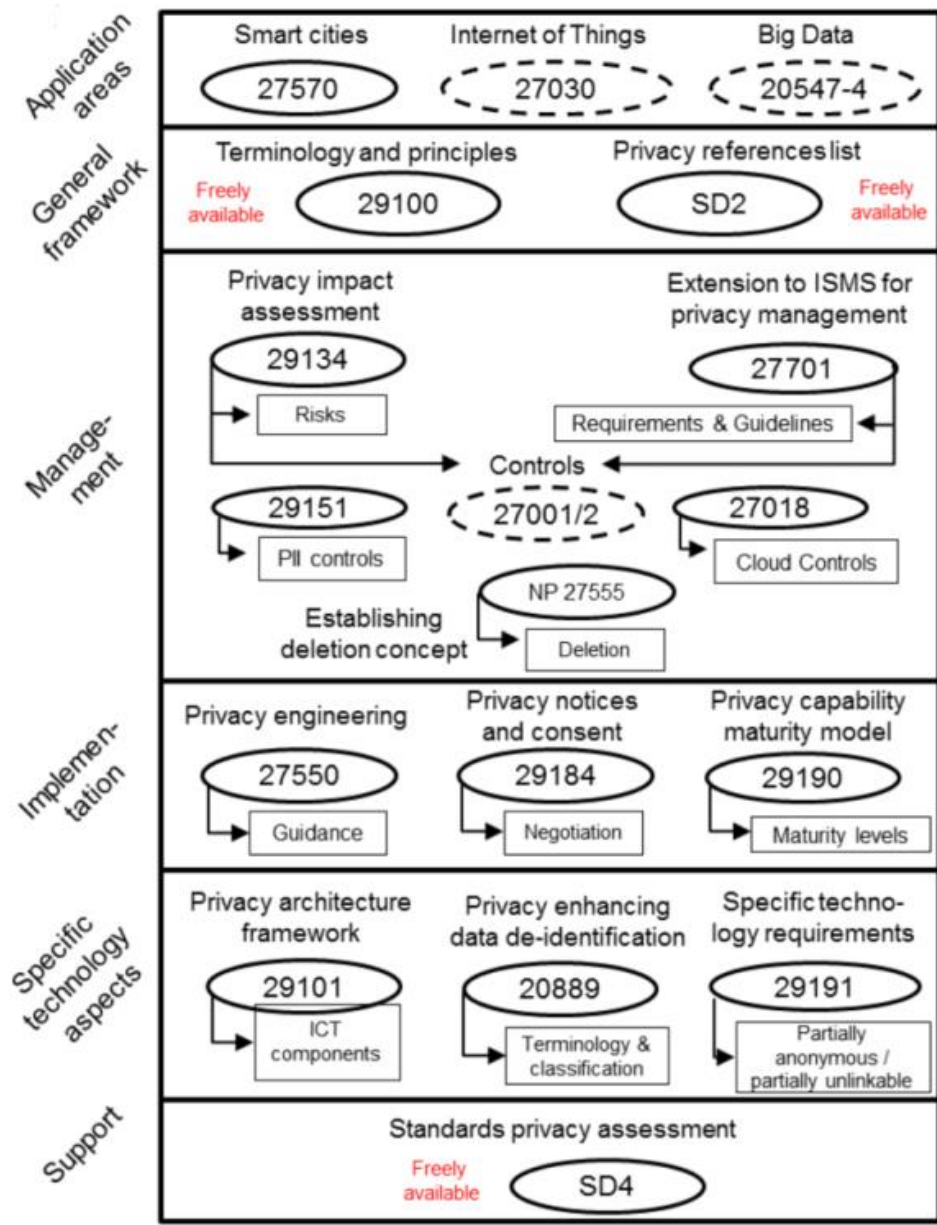
- [APP Pets \(ULD project\)](#)
- [AN.ON-Next \(ULD project\)](#)
- [CREDENTIAL \(EC project completed\)](#)
- [DNT Guide](#)
- [PARIS \(EC project completed\)](#)
- [PDP4E \(EC project on-going\)](#)
- [PRIPARE \(EC project completed\)](#)
- [PRISMACLOUD \(EC project completed\)](#)
- [Privacy framework \(NIST project on-going\)](#)
- [Privacypatterns](#)
- [Signatu](#)

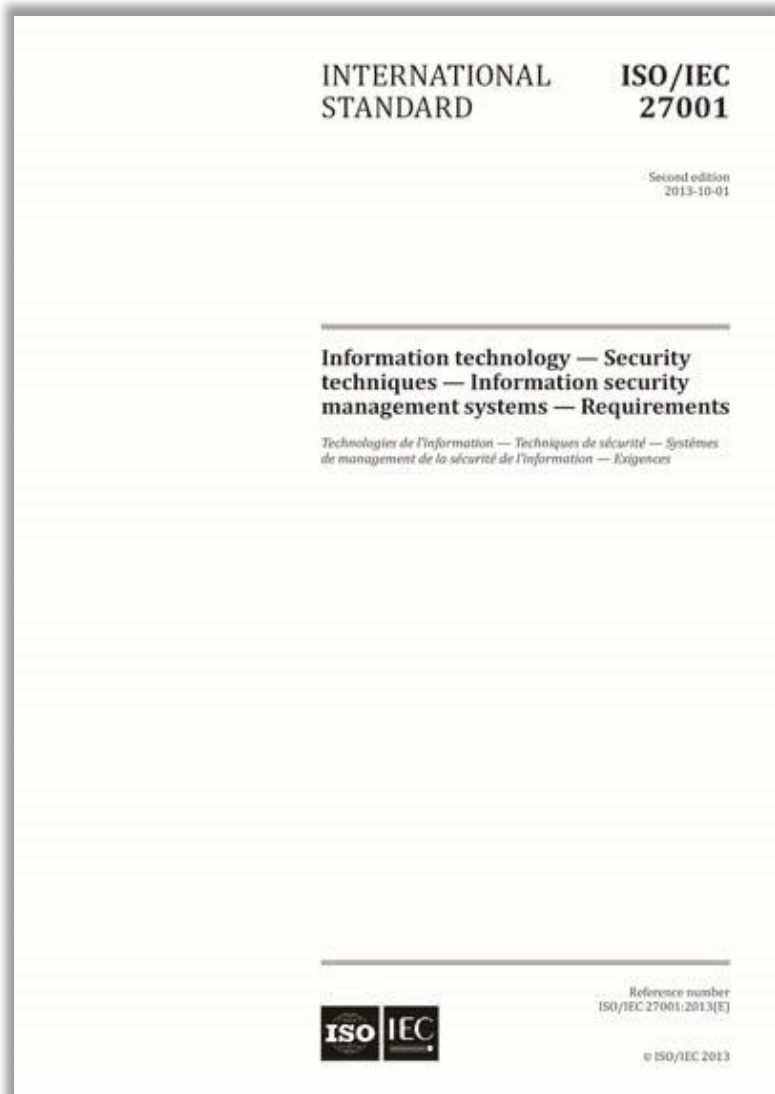
[More info on privacy engineering projects. \[Expand\]](#)

Reports, Events, Presentations

- [DPIA and PIA guidelines](#)
- [Studies](#)
- [OWASP](#)
- [Business Process Cookbook](#)
- [Events](#)
- [Presentations](#)

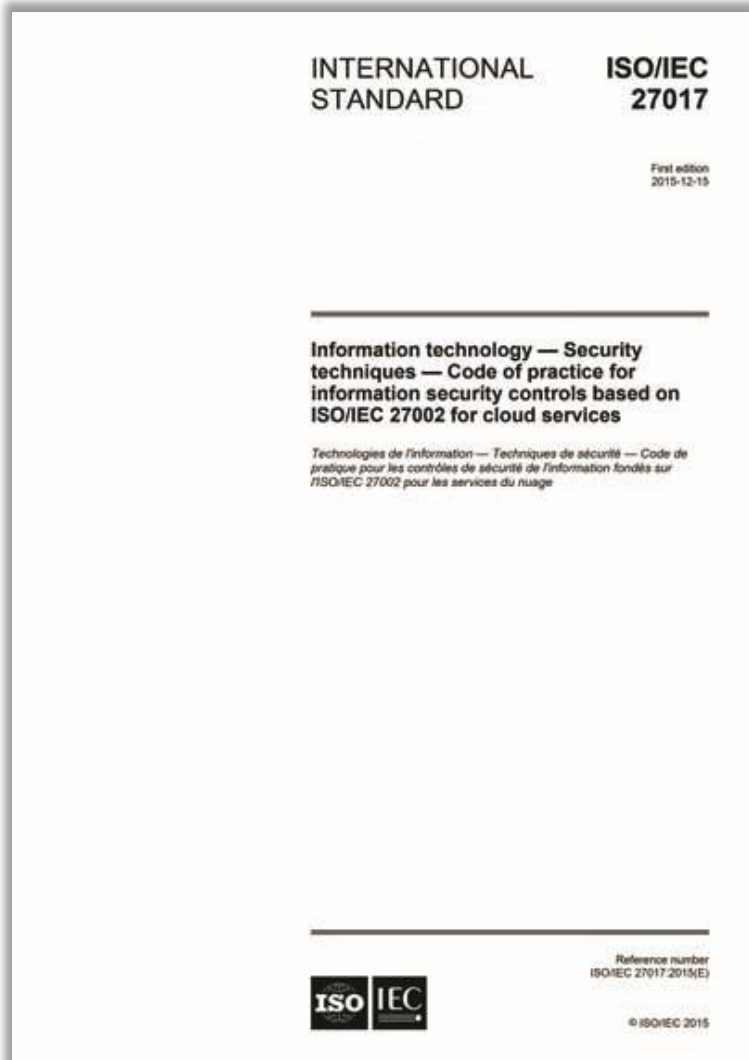
[More info on reports, events, presentations \[Expand\]](#)





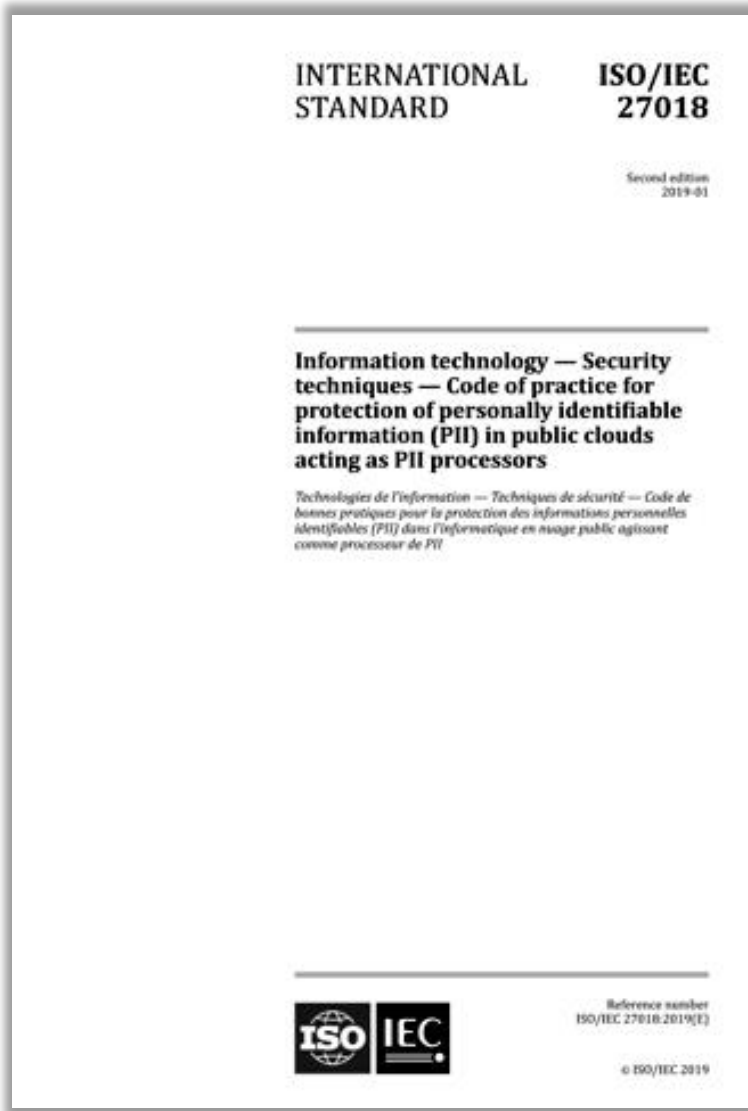
Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27001:2013 «Информационные технологии - Методы обеспечения безопасности - Системы Менеджмента Информационной Безопасности - Требования» (Information technology - Security techniques - 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).



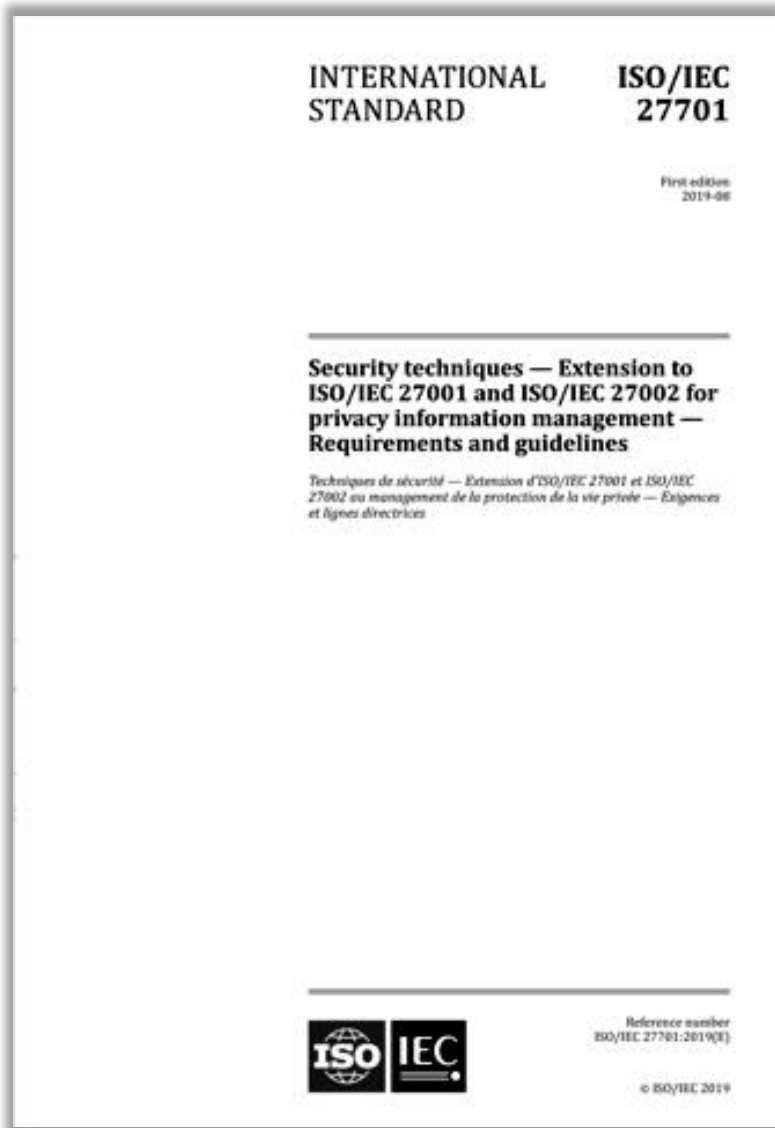
Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27017:2015 «Информационные технологии - Методы обеспечения безопасности - Система менеджмента облачной безопасности и защиты персональных данных - Меры безопасности» (Information 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.



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.



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).

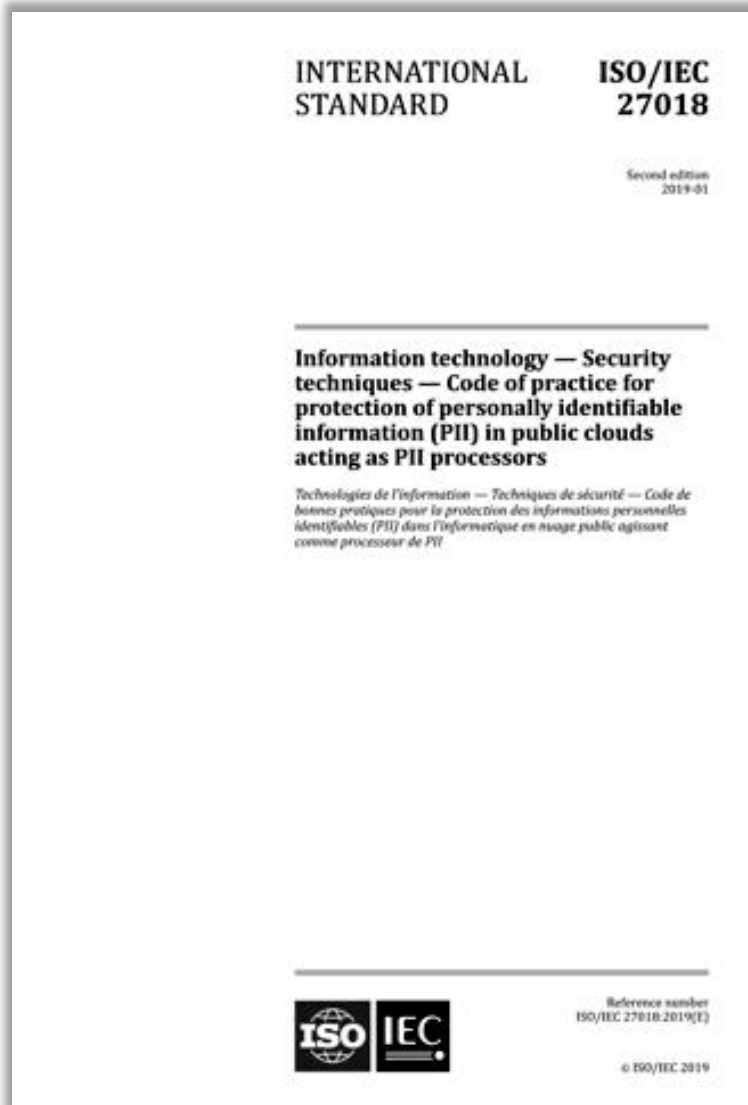
В стандарте описано руководство по созданию, внедрению, поддержанию и постоянному совершенствованию Системы управления персональными данными (Privacy Information Management System - PIMS) в контексте организации. Стандарт определяет требования, связанные с PIMS, и формулирует правила для контролеров (controllers) и обработчиков (processors) в отношении обработки персональных данных.



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).

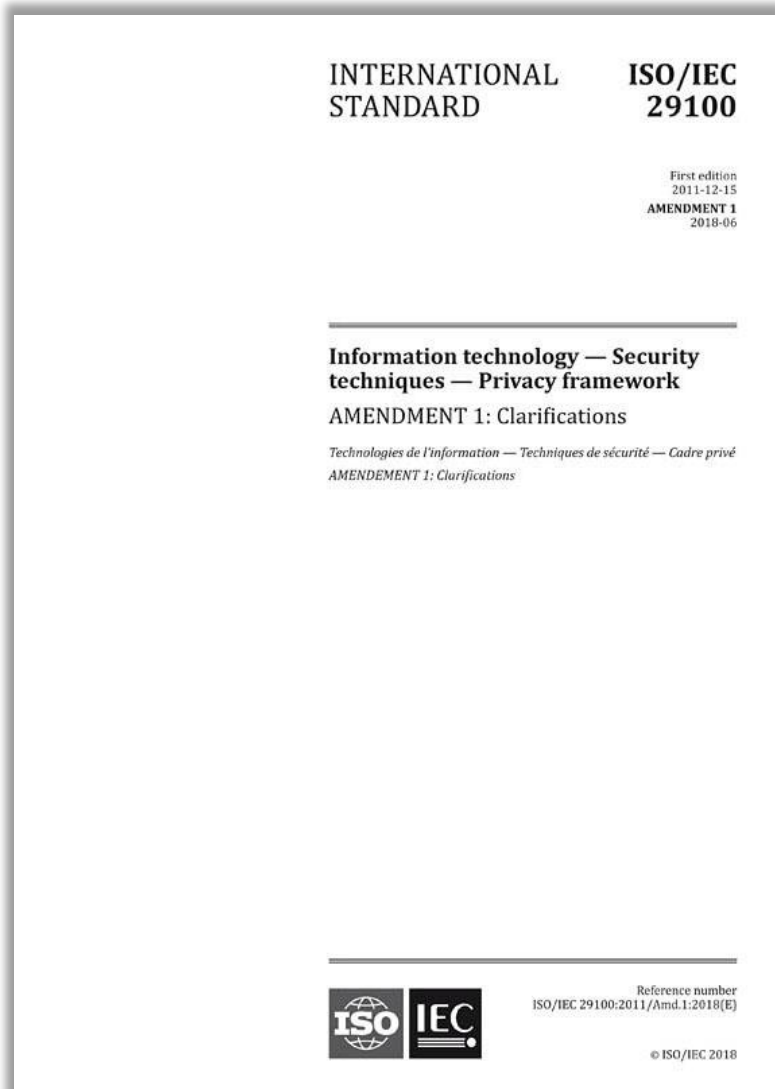
В стандарте описаны рекомендации по спроектированной защите неприкосновенности частной жизни (privacy engineering), которые призваны помочь организациям интегрировать последние достижения в сфере такого рода «встроенной» защиты в их практику проектирования систем:

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.



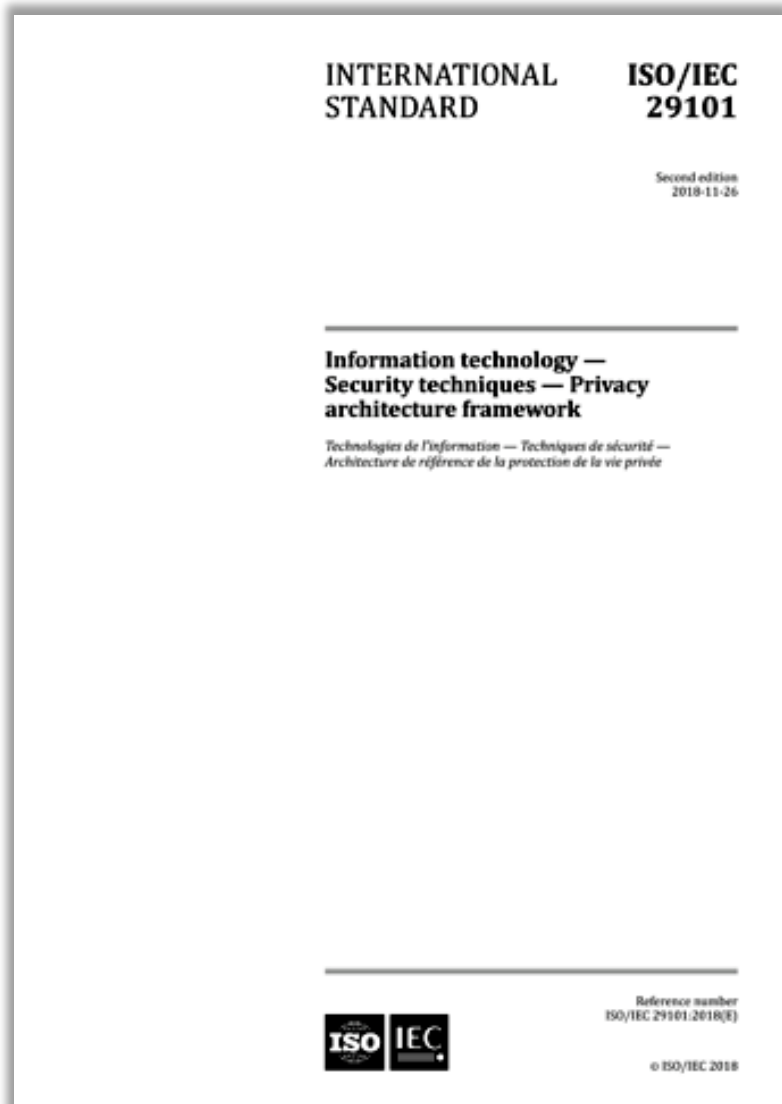
Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27102:2019 «Менеджмент информационной безопасности - Руководство по киберстрахованию» (Information security management - Guidelines for cyber-insurance).

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.



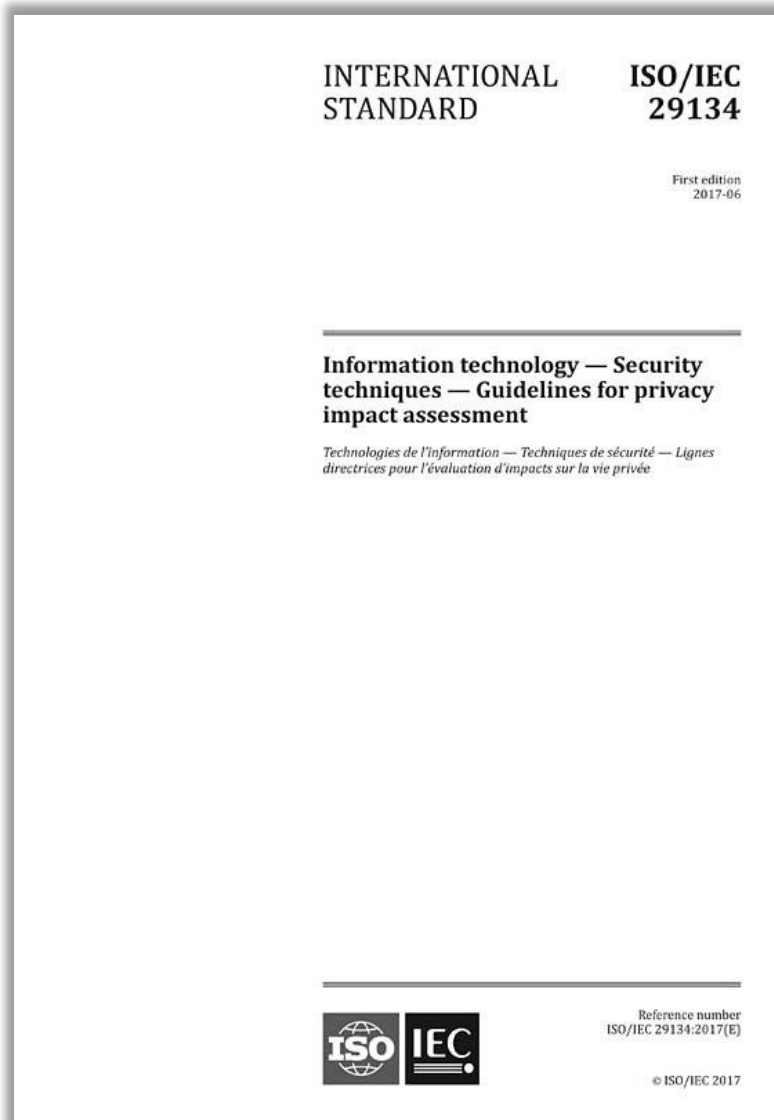
Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт 29100:2011 «Информационная технология. Методы и средства обеспечения безопасности. Концепция защиты персональных данных» (Information technology - Security techniques - Privacy framework).

В стандарте сформулированы принципы и меры по защите неприкосновенности частной жизни. В России адаптирован как ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности».



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.



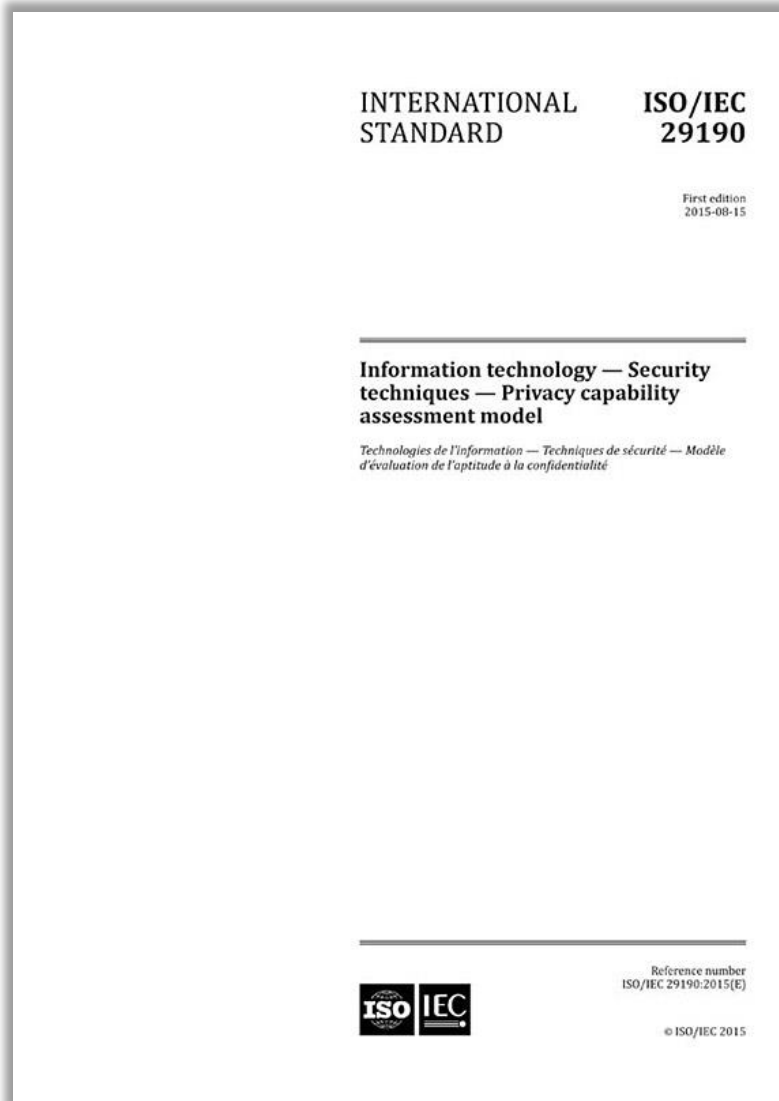
Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 29134:2017 «Информационные технологии - Методы и средства обеспечения безопасности – Оценка воздействия на неприкосновенность частной жизни – Руководство» (Information technology - 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.



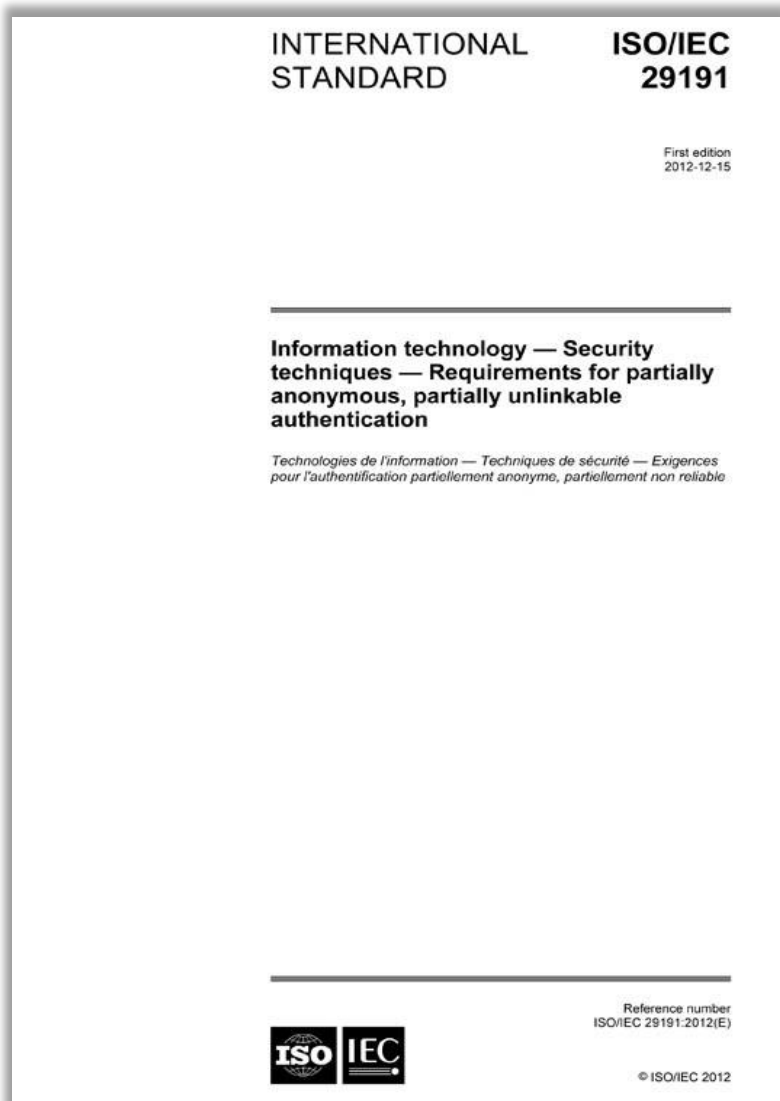
Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 29151:2017 «Информационные технологии – Методы обеспечения безопасности – Свод практики по защите персональных данных» (Information technology - Security techniques - Code of 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).



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 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.

INTERNATIONAL
STANDARD

ISO
ISO/IEC FDIS 20889

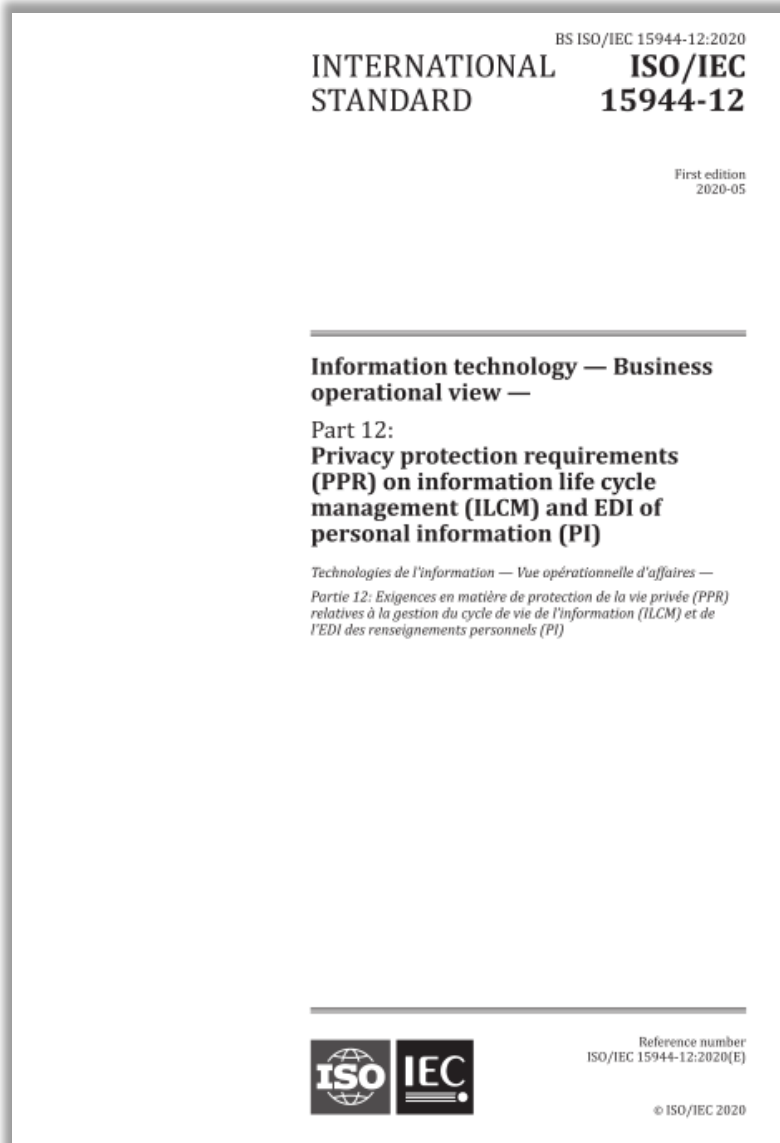
Privacy enhancing data de-identification terminology and classification of techniques



© ISO

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 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.



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.



Международной организацией по стандартизации (International Organization for Standardization) был опубликован 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.

NIST Privacy Framework: инструмент для обеспечения приватности через управление рисками в организации



Version 1.0

NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT

January 16, 2020

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way.

NIST National Institute of Standards and Technology
U.S. Department of Commerce



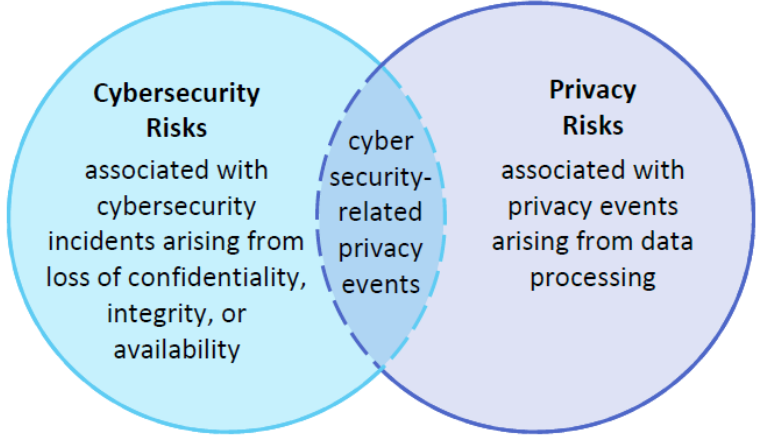
The Core provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk



Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk



Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile



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>

266 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=00000000030339453>

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

Правоприменительная практика



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"> Article 17 (Right to erasure ('right to be forgotten')) 	<ul style="list-style-type: none"> Data retention Right to erasure 	<ul style="list-style-type: none"> Reprimand 	Summary	Decision
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"> Article 24 (Responsibility of the controller) Article 32 (Security of processing) 	<ul style="list-style-type: none"> Data security Password Right of access 	<ul style="list-style-type: none"> Reprimand 	Summary	Decision
EDPBI:FR:OSS D:2020:88	20/02/2020	FR SA	LU SA	<ul style="list-style-type: none"> Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject) Article 21 (Right to object) 	<ul style="list-style-type: none"> E-Commerce Right to object 	<ul style="list-style-type: none"> Reprimand 	Summary	Decision
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"> Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject) Article 17 (Right to erasure ('right to be forgotten')) 	<ul style="list-style-type: none"> Identity verification Right to erasure User account 	<ul style="list-style-type: none"> Reprimand 	Summary	Decision

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.

DE LEGE DATA

DATENSCHUTZ – PRIVACY – WEB 2.0

HOME BLOG UND AUTOR DATENSCHUTZ-GRUNDVERORDNUNG (KONSOLIDIERTE FASS

EUDATAP – WEIHNACHTSKALENDER IMPRESSUM / DATENSCHUTZ

Austrian data protection authority: Data subjects have no right to demand implementation of certain data protection measures under GDPR

Posted on 4. NOVEMBER 2018 by CARLO PILTZ

Decisions on the GDPR (from supervisory authorities and courts) are still rare and therefore I am always very pleased when such a decision, in which the new European law is applied and interpreted, sees the light of day.

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.

CNIL.

To protect personal data, support innovation, preserve individual liberties

DATA PROTECTION | TOPICS | THE CNIL |  

Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data

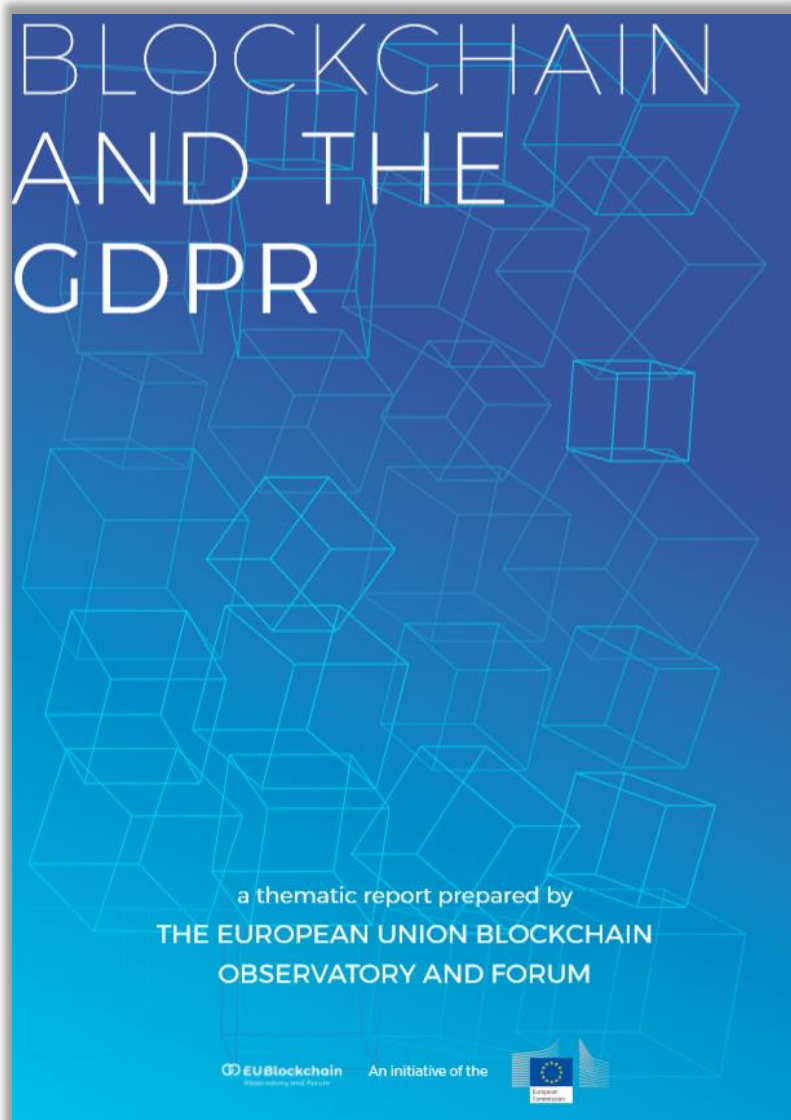
06 November 2018

Blockchain is a technology with a high potential for development that raises many questions, including questions on its compatibility with the GDPR. For this reason, the CNIL has addressed this matter and presents concrete solutions to stakeholders who wish to use it as part of their personal data processing operations.

Commission nationale de l'informatique et des libertés

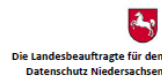
Французский надзорный орган CNIL опубликовал отчет о специфике и особенностях использования технологии блокчейн в контексте обработки персональных данных и соблюдения требований GDPR.

BLOCKCHAIN



Contents

4	Executive summary	
7	Introduction	
10	Evolution from above: Introduction to the GDPR	
	Personal data, the heart of the GDPR	10
	GDPR roles	11
	Principles, rights and obligations	12
14	Revolution from below: Blockchain and the tools of decentralisation	
	The decentralized database model	14
	Public blockchains and permissioned blockchains	14
	Is there a GDPR-compliant blockchain?	16
17	Tensions between the GDPR and blockchain	
	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	Opposites attract: Resolving the tensions between blockchain and the GDPR	
32	Appendix	
	Blockchain terminology	32
	Infographic	35



Abschlussbericht November 2019

Querschnittsprüfung der LfD Niedersachsen von 50 Unternehmen zur Umsetzung der seit dem 25. Mai 2018 unmittelbar geltenden Datenschutz-Grundverordnung (EU) 2016/679 (DS-GVO)

Abschlussbericht zur Querschnittsprüfung in Unternehmen / November 2019

1

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.



Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Pressemitteilung

711.424.1

17. Juli 2020

Nach „Schrems II“: Europa braucht digitale Eigenständigkeit

Nach der Entscheidung des Europäischen Gerichtshofs (EuGH), das „EU-US Privacy Shield“ für ungültig zu erklären, fordert die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Maja Smoltczyk, datenverarbeitende Stellen in Berlin auf, in den USA gespeicherte personenbezogene Daten nach Europa zu verlagern.

Der EuGH hat in seiner Entscheidung „Schrems II“ (C-311/18) am Donnerstag, dem 16. Juli 2020, festgestellt, dass US-Behörden zu weitreichende Zugriffsmöglichkeiten auf Daten europäischer Bürgerinnen und Bürger haben. Daraus folgt, dass personenbezogene Daten bis zu einer Änderung der Rechtslage in aller Regel nicht mehr wie bisher in die USA übermittelt werden dürfen. Ausnahmen bestehen vor allem in den gesetzlich vorgesehenen Sonderfällen, etwa bei einer Hotelbuchung in den USA.

Der EuGH stellt unter anderem fest, dass in den USA staatliche Überwachungsmaßnahmen bestehen, die mit einer massenhaften Sammlung personenbezogener Daten ohne klare Beschränkungen einhergehen. Dies widerspreche der EU-Grundrechtecharta (Rn. 180 ff. des Urteils). Weiter stellt er fest, dass europäische Bürgerinnen und Bürger keine Möglichkeit haben, Überwachungsmaßnahmen von US-Behörden gerichtlich überprüfen zu lassen. Dadurch sei der Wesensgehalt des europäischen Grundrechts auf effektiven Rechtsschutz verletzt.

Übermittlungen personenbezogener Daten in Drittländer sind nur dann zulässig, wenn diese ein Datenschutzniveau aufweisen, das den europäischen Grundrechten der Sache nach gleichwertig ist. Da dies nach den Feststellungen des höchsten europäischen Gerichts in den USA weitgehend nicht der Fall ist, erklärt der EuGH in seiner Entscheidung das „EU-US Privacy Shield“ für ungültig, auf dessen Grundlage eine Übermittlung personenbezogener Daten in die USA bisher in vielen Fällen erfolgte. Die sogenannten Standardvertragsklauseln, die europäische Unternehmen mit Anbietern in Drittländern abschließen können, um das europäische Datenschutzniveau auch in den Drittländern zu wahren, erklärt der EuGH dagegen unter bestimmten Bedingungen für grundsätzlich zulässig. Er betont in diesem Zusammenhang jedoch, dass sowohl die europäischen Datenexporteure als auch die Datenimporteure in Drittländern verpflichtet sind, vor der ersten Datenübermittlung zu prüfen, ob im Drittland staatliche Zugriffsmöglichkeiten auf die Daten bestehen, die über das nach europäischem Recht Zulässige hinausgehen (Rn. 134 f., 142 des Urteils). Bestehen solche Zugriffsrechte, können auch die Standardvertragsklauseln den Datenexport nicht rechtfertigen. Bereits ins Drittland übermittelte Daten müssen zurückgeholt werden. Anders als bisher verbreitet vertreten, genügt der reine Abschluss von Standardvertragsklauseln nicht, um Datenexporte zu ermöglichen (Rn. 126 ff. des Urteils).

Pressesprecherin: Dalia Kues
Geschäftsstelle: Cristina Vecchi
E-Mail: presse@datenschutz-berlin.de

Friedrichstr. 219
10000 Berlin
Tel: 030 13889 - 900
Fax: 030 2156050



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.

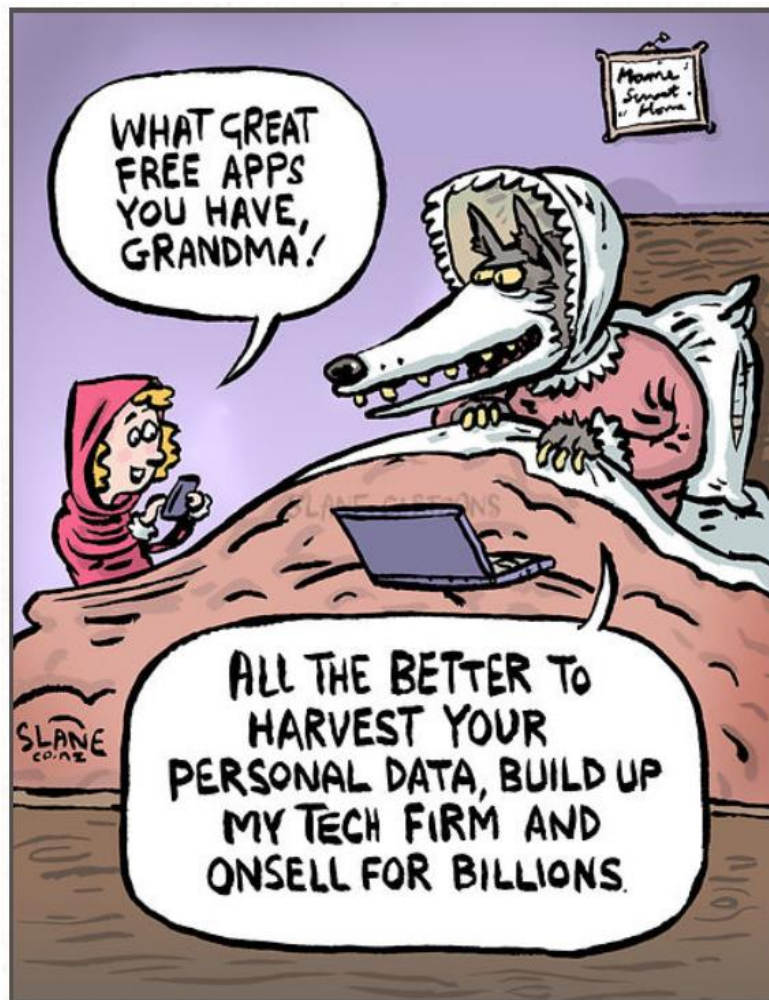
5 MOST COMMON GDPR MISTAKES

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.

Штрафы - базы дел и аналитика



GDPR Enforcement Tracker






Общедоступная онлайн-база сведений об известных случаях привлечения к юридической ответственности за нарушение GDPR. База регулярно актуализируется.

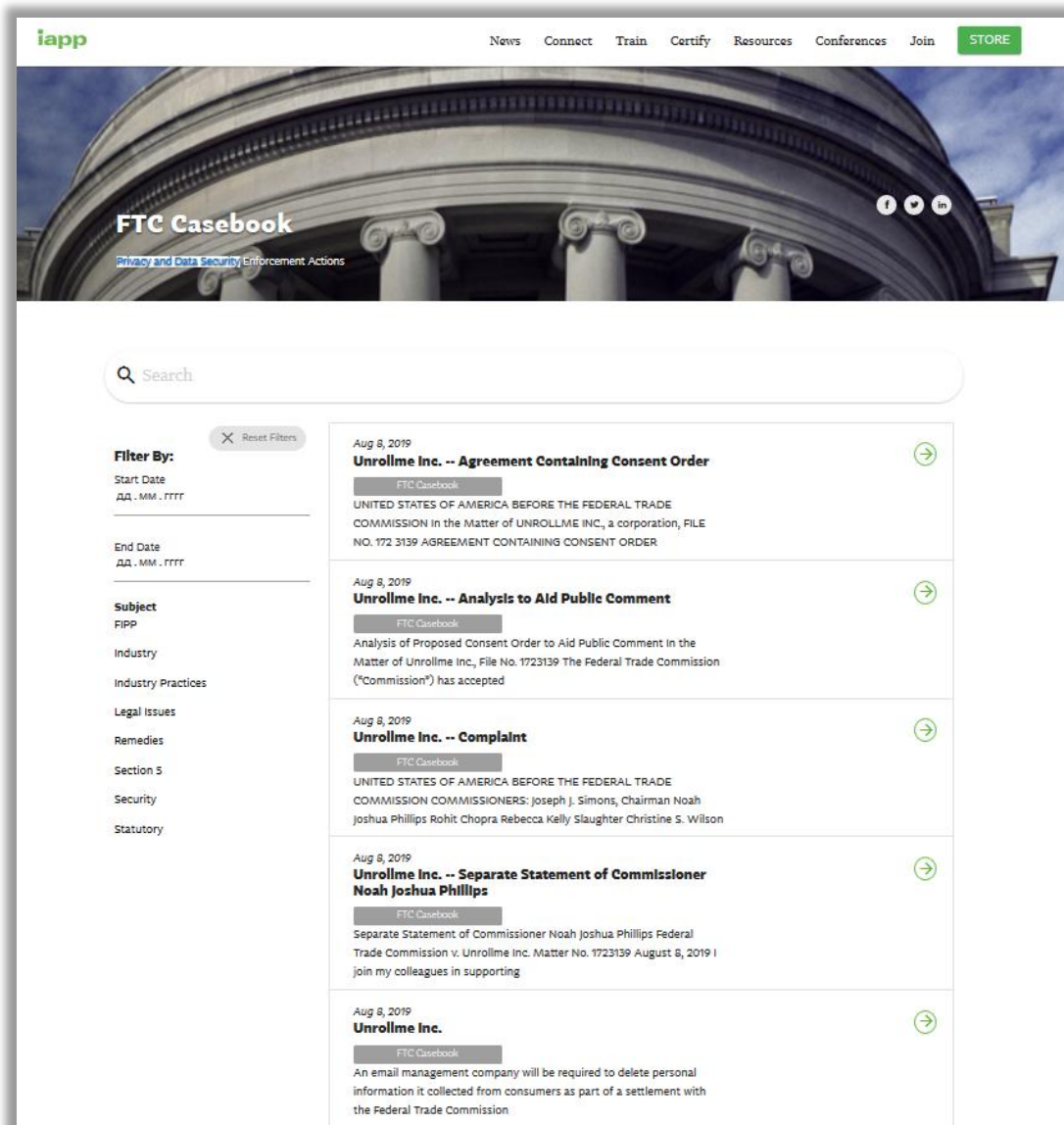
tracked by **C/M'S**
Law.Tax

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 460k EUR: [link](#) The ICO issued a notice of its intention to fine British Airways GBP 183.39 Mio for GDPR infringements (no final decision): [link](#) First fine aga

Show entries Search:

Country	Authority	Date	Fine	Controller/Processor	Quoted Article	Summary	Infos
 UNITED KINGDOM	Information Commissioner (ICO)	2019-07-08	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 £183.39M 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 name and address information.	link
 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 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.	link
 FRANCE	French Data Protection Authority (CNIL)	2019-01-21	50,000,000	Google Inc.	Art. 13 GDPR, Art. 14 GDPR, Art. 6 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 25th and 28th 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).	link
 BULGARIA	Data Protection Commission of Bulgaria (KZLD)	2019-08-28	2,600,000	National Revenue Agency	Art. 32 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.	link
 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 23000 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.	link



The screenshot displays the IAPP website's 'FTC Casebook' section. The page features a search bar at the top, a navigation menu with links like 'News', 'Connect', 'Train', 'Certify', 'Resources', 'Conferences', and 'Join', and a 'STORE' button. The main content area is titled 'FTC Casebook' and includes a sub-header 'Privacy and Data Security Enforcement Actions'. A search bar is present, and a 'Filter By' sidebar on the left lists categories such as 'Start Date', 'End Date', 'Subject', 'Industry', 'Legal Issues', 'Remedies', 'Section 5', 'Security', and 'Statutory'. The main list shows five entries, all dated 'Aug 8, 2019', each with a green arrow icon to the right. The entries are:

- Unrollme Inc. -- Agreement Containing Consent Order**: 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
- Unrollme Inc. -- Analysis to Aid Public Comment**: 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
- Unrollme Inc. -- Complaint**: UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION COMMISSIONERS: Joseph J. Simons, Chairman Noah Joshua Phillips Rohit Chopra Rebecca Kelly Slaughter Christine S. Wilson
- Unrollme Inc. -- Separate Statement of Commissioner Noah Joshua Phillips**: 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
- Unrollme Inc.**: 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.

Количество штрафов: 110

Источники: надзорные органы (DPA), EDPB, IAPP

Условия:

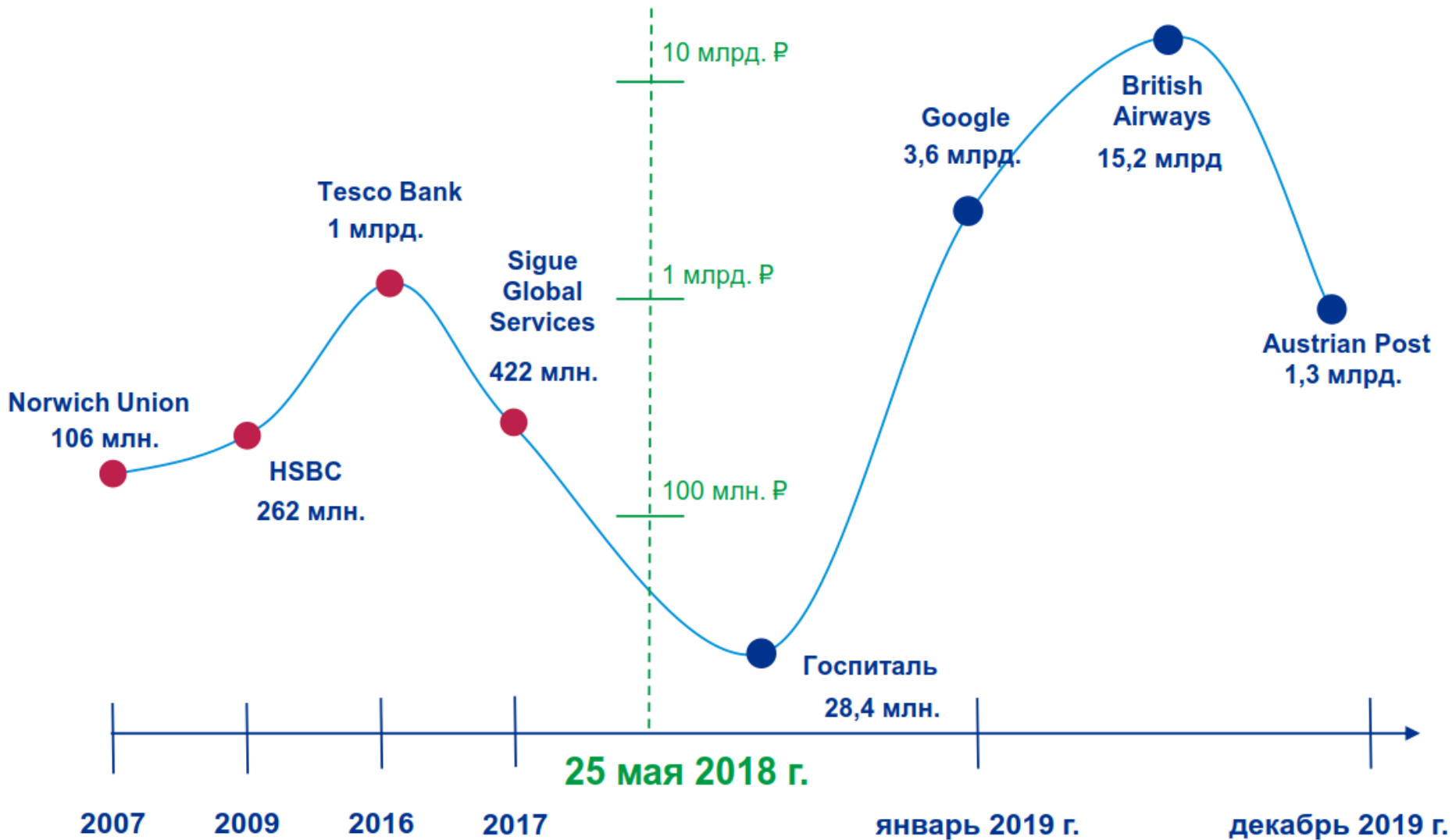
Германия, Австрия, Кипр – не публикуют на сайте надзорного органа предписания, но в открытых источниках есть сведения, что были постановления о штрафах (в аналитике учитывались только штрафы, освещенные EDPB или IAPP).

Чехия, Венгрия, Португалия – надзорные органы публикуют предписания по штрафам анонимно (анонимные штрафы учитывались в аналитике).

Курс валют*: по данным ЦБ на 03 декабря 2019 г.

* Размер штрафа в рублях рассчитывался конвертацией из валюты, в которой был выписан штраф, в рубли по курсу ЦБ

Наименование	Страна
National Authority for Data Protection and Freedom of Information	Венгрия
Agencia de Protección de Datos	Испания
The Office for Personal Data Protection	Чехия
Commission for Personal Data Protection	Болгария
The National Supervisory Authority for Personal Data Processing	Румыния
Österreichische Datenschutzbehörde	Австрия
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	Германия
Commission Nationale de l'Informatique et des Libertés – CNIL	Франция
The Bureau of the Inspector General for the Protection of Personal Data	Польша
Comissão Nacional de Protecção de Dados – CNPD	Португалия
The Information Commissioner's Office	Великобритания
Hellenic Data Protection Authority	Греция
Commission de la protection de la vie privée	Бельгия
Datatilsynet	Дания
Datatilsynet	Норвегия
Garante per la protezione dei dati personali	Италия
Data State Inspectorate	Латвия
State Data Protection	Литва
Office of the Data Protection Commissioner	Мальта
Autoriteit Persoonsgegevens	Нидерланды
Datainspektionen	Швеция
European Data Protection Board - EDPB	Все
International Association of Privacy Professionals - IAPP	Все



Страны, входящие в ЕЭЗ, в которых зафиксированы штрафы

На 8 ноября

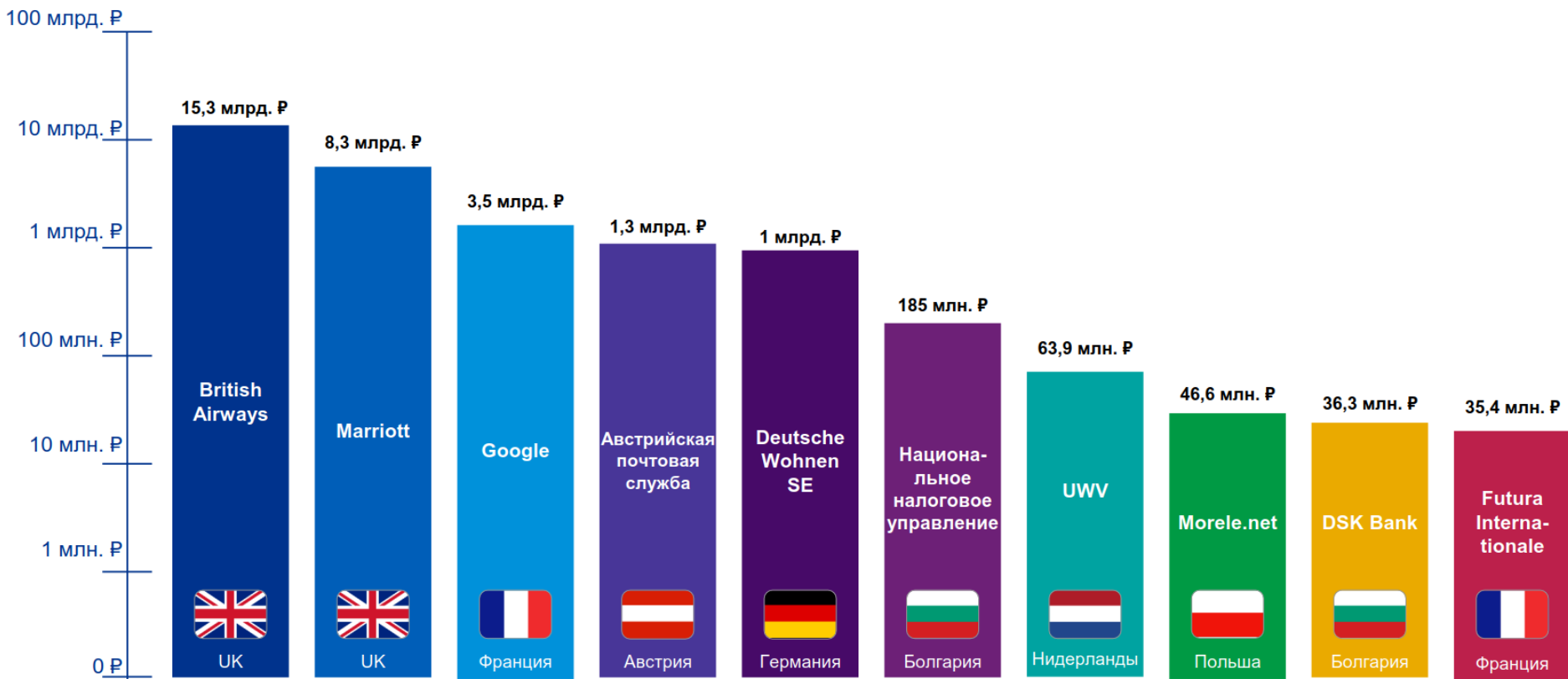
Страна	Штрафы	Общая сумма (₽)
Венгрия	17	13 398 000
Испания	17	56 710 352
Чехия	9	1 246 500
Болгария	7	222 654 260
Румыния	7	23 390 221
Австрия	5	1 282 965 169
Германия	5	1 046 755 401
Франция	4	3 594 118 000
Польша	4	63 995 906
Португалия	3	29 974 660
Великобритания	2	23 421 092 020
Греция	2	39 066 500
Бельгия	2	852 360
Дания	2	25,677 000
Норвегия	2	24 948 000
Италия	1	3 551 500
Латвия	1	497 210
Литва	1	4 368 345
Мальта	1	355 150
Нидерланды	1	32 673 800
Швеция	1	1 316 000
ИТОГО	94	29 889 606 355

На 3 декабря

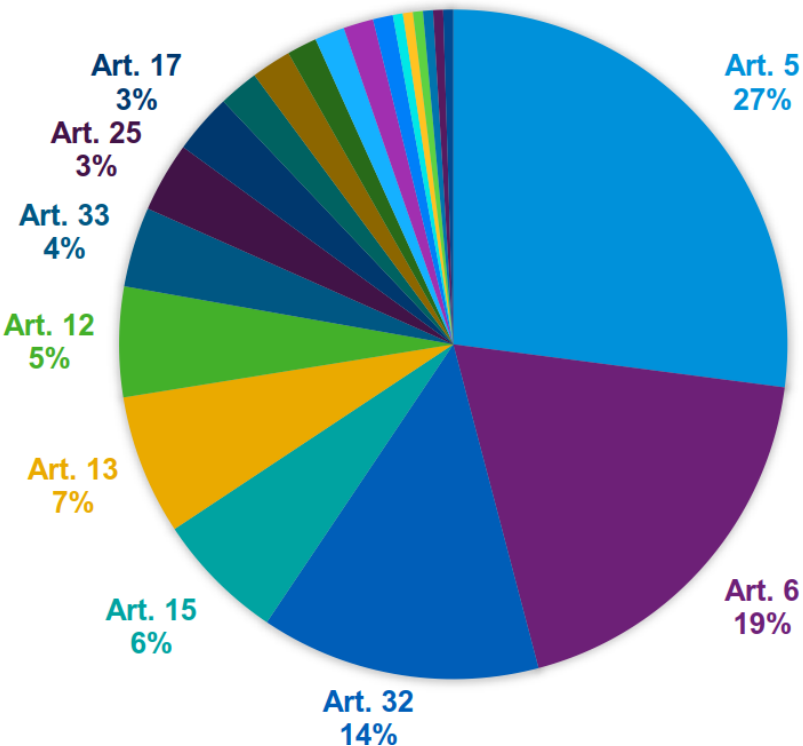
Страна	Штрафы	Общая сумма (₽)
Испания	25	72 378 265
Венгрия	17	12 928 217
Румыния	12	31 567 515
Чехия	9	1 250 001
Болгария	7	223 733 927
Австрия	5	1 281 935 618
Германия	5	1 045 915 403
Франция	5	3 626 720 300
Польша	5	67 001 753
Португалия	3	29 950 606
Великобритания	2	23 518 246 599
Греция	2	39 035 150
Бельгия	2	851 676
Дания	2	25 646 085
Норвегия	2	25 233 156
Нидерланды	2	96 523 280
Италия	1	3 548 650
Латвия	1	496 811
Литва	1	4 364 840
Мальта	1	354 865
Швеция	1	1 345 864
ИТОГО	110	30 109 028 581

Доля штрафов по странам (по количеству)

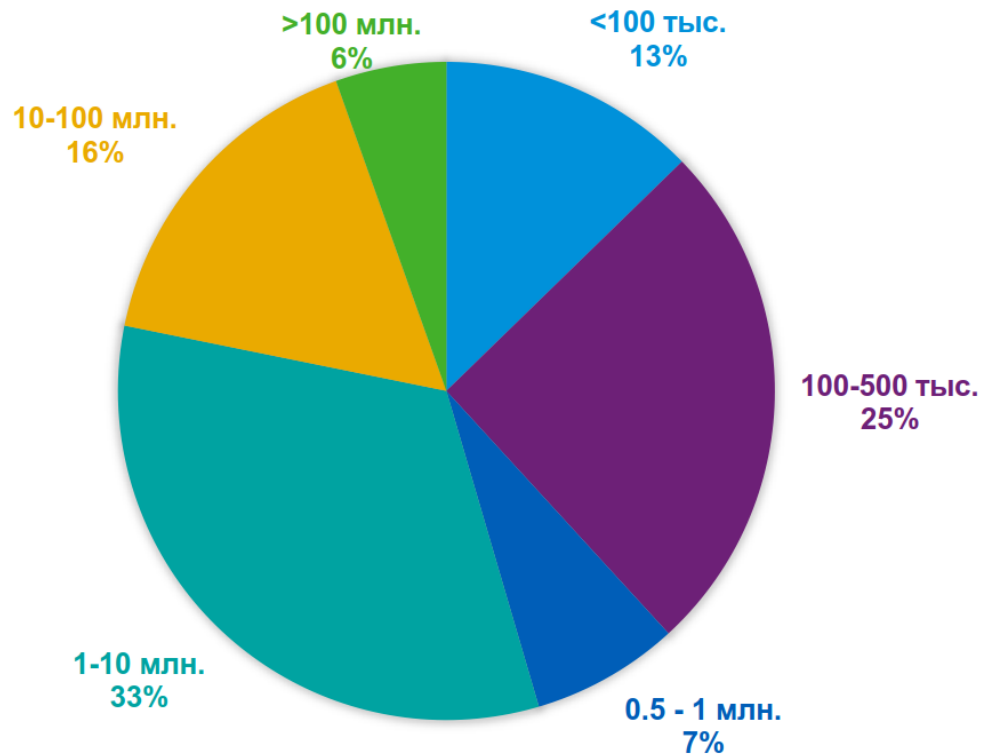




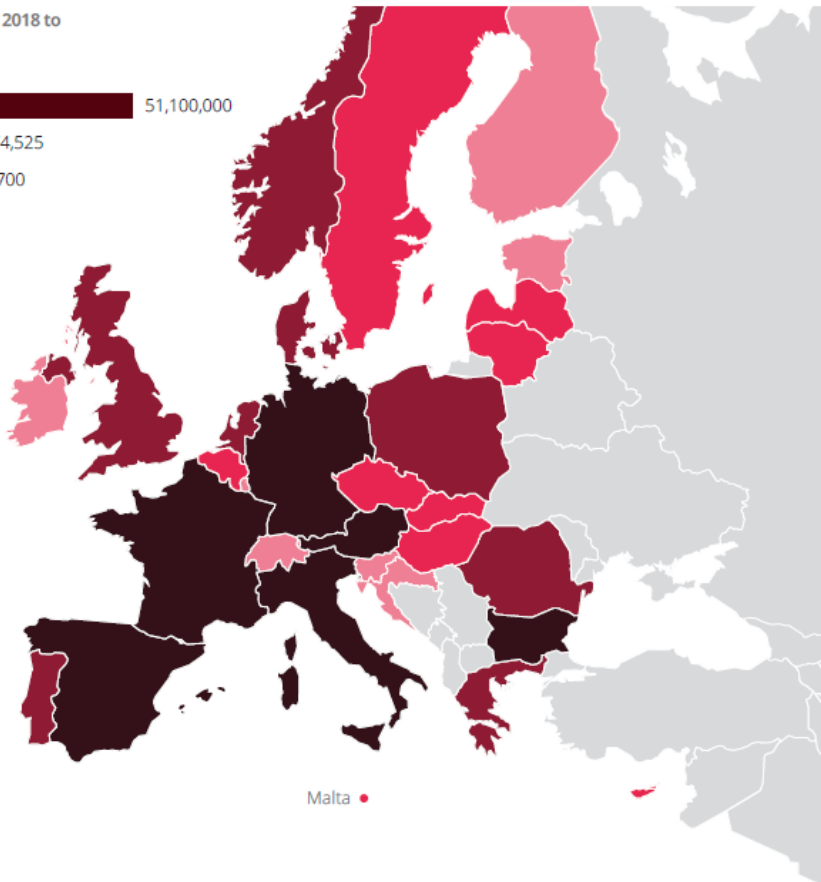
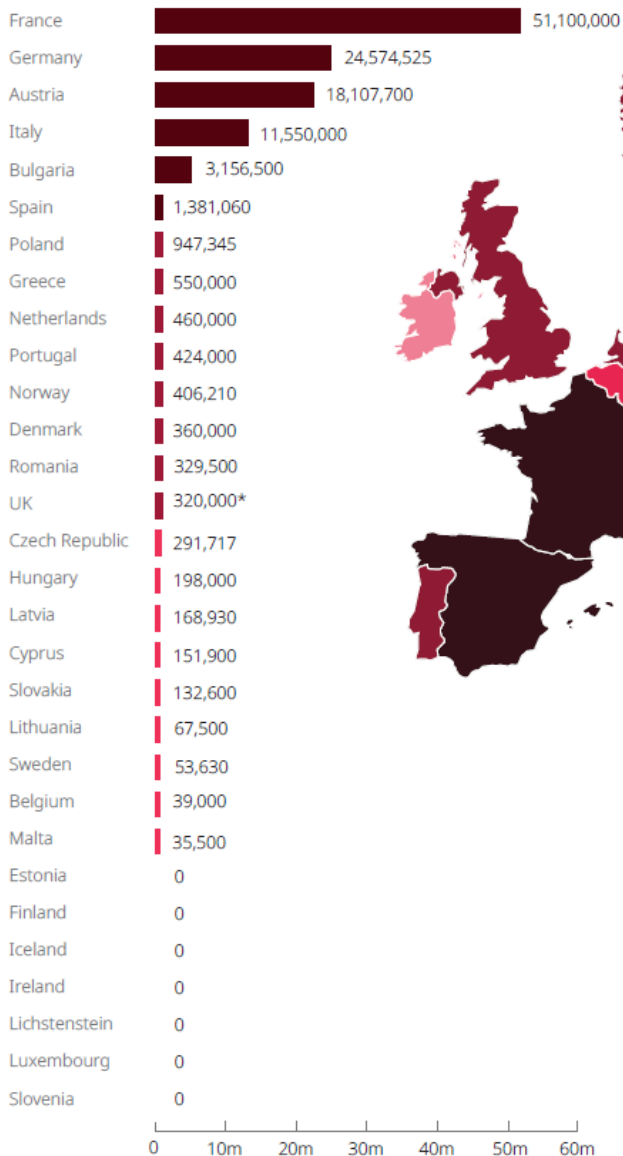
Доли штрафов по статьям



Доли штрафов по размеру (руб.)



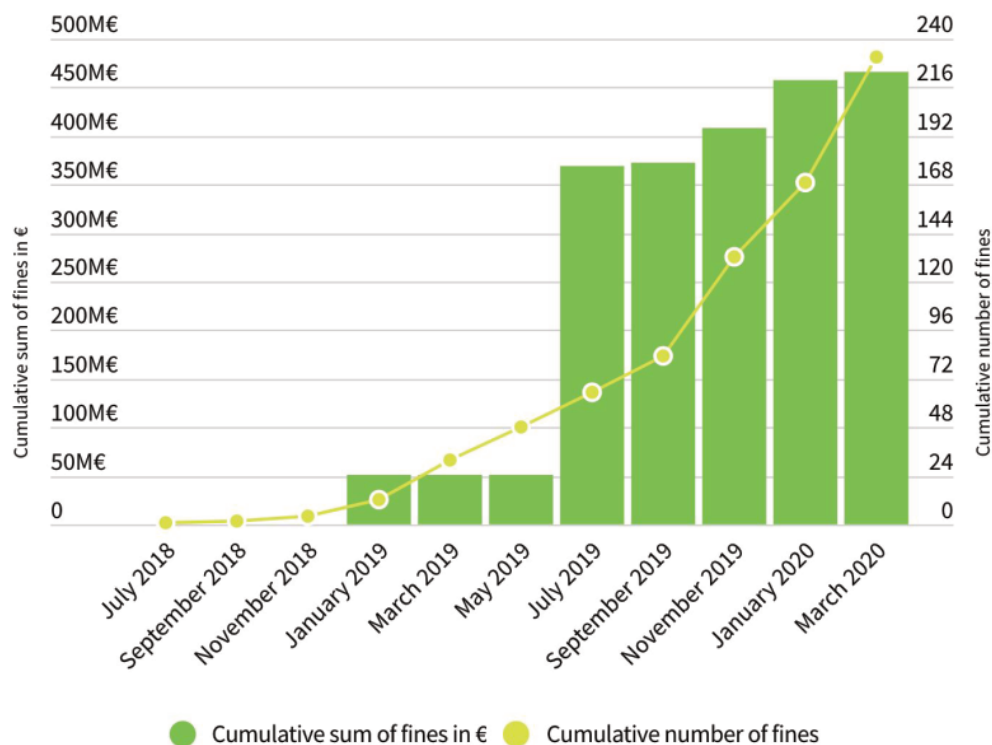
Total value of GDPR fines imposed from 25 May 2018 to 17 January 2020 in Euros



- Aggregate fines more than 1 million Euros
- Aggregate fines between 300,000 and 1 million Euros
- Aggregate fines up to 300,000 Euros
- No fines reported

*The UK figures do not include the two public notices of intent to fine totalling £282 million (about €329 million / \$366 million) as they had not been finalised and imposed at the time of writing this report.

How many fines were given under the GDPR?



Top 10 fines given under the GDPR

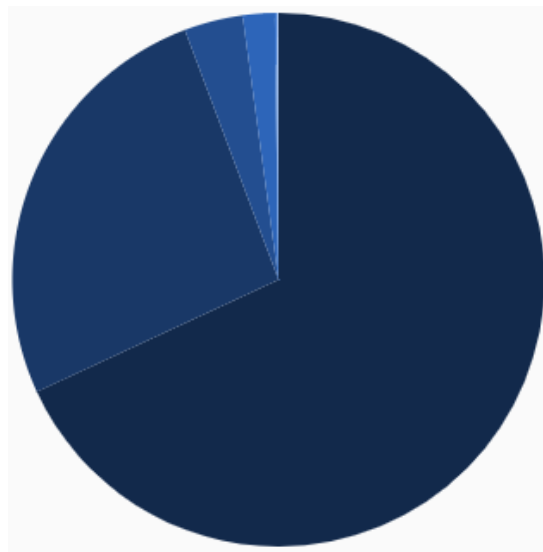
COMPANY	AMOUNT IN €
British Airways	204,600,000 €
Marriott International	110,390,200 €
Google Inc	50,000,000 €
TIM	27,800,000 €
Austrian Post	18,000,000 €
Deutsche Wohnen SE	14,500,000 €
1&1 Telecom GmbH	9,550,000 €
Eni Gas e Luce	8,500,000 €
Google LLC	7,000,000 €
Eni Gas e Luce	3,000,000 €

Сводная статистика по объемам штрафов за нарушение GDPR к сентябрю 2020 года

Country	2018	2019	2020	Grand Total
AUSTRIA	9 100 €	18 061 000 €	100 €	18 070 200 €
BELGIUM		39 000 €	720 000 €	759 000 €
BULGARIA	500 €	3 197 960 €	12 230 €	3 210 690 €
CROATIA			0 €	0 €
CYPRUS		111 000 €	10 000 €	121 000 €
CZECH REPUBLIC	5 096 €	14 270 €		19 366 €
DENMARK		360 850 €	202 300 €	563 150 €
ESTONIA			548 €	548 €
FINLAND			207 500 €	207 500 €
FRANCE		51 100 000 €	250 000 €	51 350 000 €
GERMANY	45 618 €	25 092 307 €	1 240 000 €	26 377 925 €
GREECE		720 000 €	36 000 €	756 000 €
HUNGARY	3 200 €	214 697 €	299 860 €	517 757 €
ICELAND			29 600 €	29 600 €
IRELAND			115 000 €	115 000 €
ISLE OF MAN			13 500 €	13 500 €
ITALY		11 550 000 €	45 672 000 €	57 222 000 €
LATVIA		157 000 €		157 000 €
LITHUANIA		61 500 €		61 500 €
MALTA		5 000 €		5 000 €
NORWAY		290 000 €	742 060 €	1 032 060 €
POLAND		934 330 €	68 600 €	1 002 930 €
PORTUGAL	400 000 €	24 000 €		424 000 €
ROMANIA		484 500 €	57 650 €	542 150 €
SLOVAKIA	90 000 €			90 000 €
SPAIN	183 600 €	1 134 500 €	2 291 310 €	3 609 410 €
SWEDEN		53 630 €	7 031 800 €	7 085 430 €
THE NETHERLANDS		1 410 000 €	2 080 000 €	3 490 000 €
UNITED KINGDOM		315 310 200 €		315 310 200 €
Grand Total	737 114 €	430 325 744 €	61 080 058 €	492 142 916 €

Country	2018	2019	2020	Total
Austria	5	3	1	8
Belgium		6	8	14
Bulgaria	1	15	4	20
Croatia			1	1
Cyprus		6	2	8
Czech Republic	4	7		11
Denmark		2	6	8
Estonia			2	2
France		5	1	6
Germany	5	20	1	26
Greece		5	5	10
Hungary	1	21	7	29
Iceland			2	2
Ireland			2	2
Isle of Man			1	1
Italy		3	22	25
Latvia		2		2
Lithuania		1		1
Malta		1		1
Netherlands		3	3	6
Norway		2	8	10
Poland		5	6	11
Portugal	1	3		4
Romania		21	15	36
Slovakia	6			6
Spain	7	31	90	128
Sweden		2	4	6
UK		3		3
Grand Total	29	167	196	392

Violation	Sum of Fines
Insufficient technical and organisational measures to ensure information security	€ 335,197,807 (at 81 fines)
Insufficient legal basis for data processing	€ 128,792,540 (at 152 fines)
Non-compliance with general data processing principles	€ 17,550,565 (at 61 fines)
Insufficient fulfilment of data subjects rights	€ 9,534,197 (at 41 fines)
Insufficient fulfilment of information obligations	€ 568,305 (at 20 fines)
Insufficient fulfilment of data breach notification obligations	€ 220,725 (at 9 fines)
Lack of appointment of data protection officer	€ 136,000 (at 4 fines)
Insufficient cooperation with supervisory authority	€ 135,211 (at 15 fines)
Insufficient data processing agreement	€ 14,380 (at 2 fines)
Insufficient cooperation with supervisory authority	€ 4,400 (at 1 fines)
Unknown	€ 500 (at 1 fines)
Insufficient fulfilment of data breach obligations	€ 286 (at 1 fines)



The Register®

Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH

Year 1 of GDPR: Over 200,000 cases reported, firms fined €56 meeelli... Oh, that's mostly Google

2019 just a transition year, says French watchdog


By Rebecca Hill 14 Mar 2019 at 09:56 27 SHARE ▼



European data protection agencies have issued fines totalling €56m for GDPR breaches since it was enforced last May, from more than 200,000 reported cases – but watchdogs have said they're just warming up.

Регуляторы из Великобритании, Норвегии и Нидерландов уже разрабатывают непубличные правила определения размера взыскания. В документе будут собраны факторы, влияющие на сумму штрафа: длительность инцидента, скорость реакции компании, количество пострадавших от утечки.

Голландский регулятор (Autoriteit Persoonsgegevens) первым в ЕС опубликовал методику расчета и наложения штрафов за нарушения требований законодательства о персональных данных, включая GDPR.



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 39c van de Wet politiegegevens, artikelen 27, 39r, 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 boetebandbreedtes

- 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 boetebandbreedtes:

Categorie	Boetebandbreedte	Basisboete
Categorie I	Boetebandbreedte tussen € 0 en € 200.000	Basisboete: € 100.000
Categorie II	Boetebandbreedte tussen € 120.000 en € 500.000	Basisboete: € 310.000
Categorie III	Boetebandbreedte tussen € 300.000 en € 750.000	Basisboete: € 525.000
Categorie IV	Boetebandbreedte 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.

Category	Standard fine bandwidth	Standard penalty
I	EUR 0 – 200.000	EUR 100.000
II	EUR 120.000 – 500.000	EUR 310.000
III	EUR 300.000 – 750.000	EUR 525.000
IV*	EUR 450.000 – 1.000.000	EUR 725.000
* Only in case the legal maximum penalty of EUR 20.000.000/ 4% turnover applies.		

STEP
1

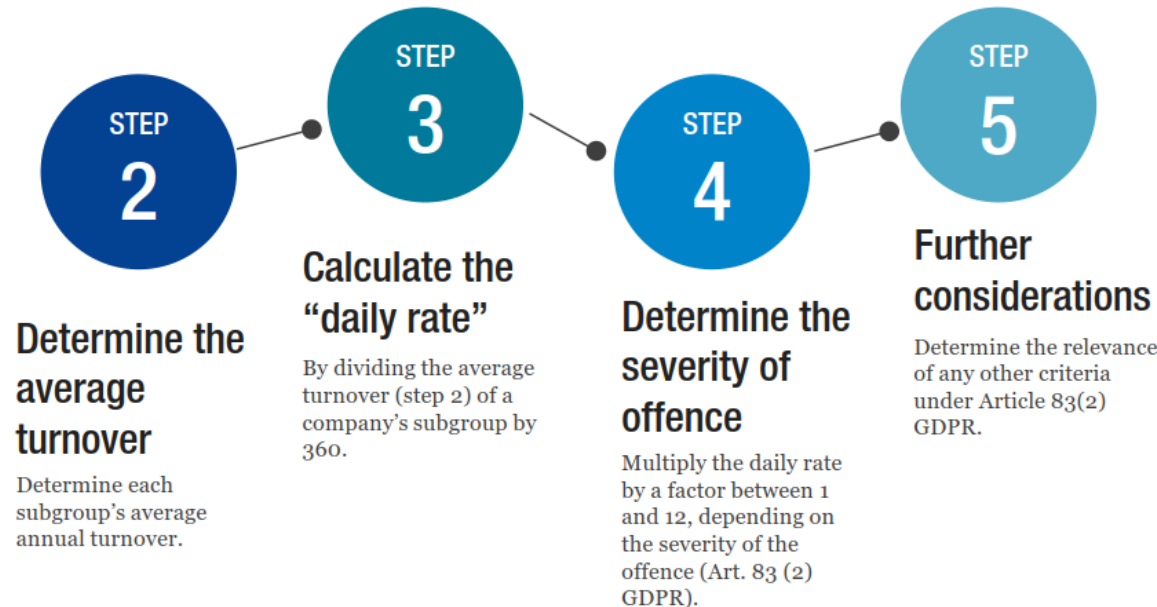
Classify company by size

By global annual turnover.

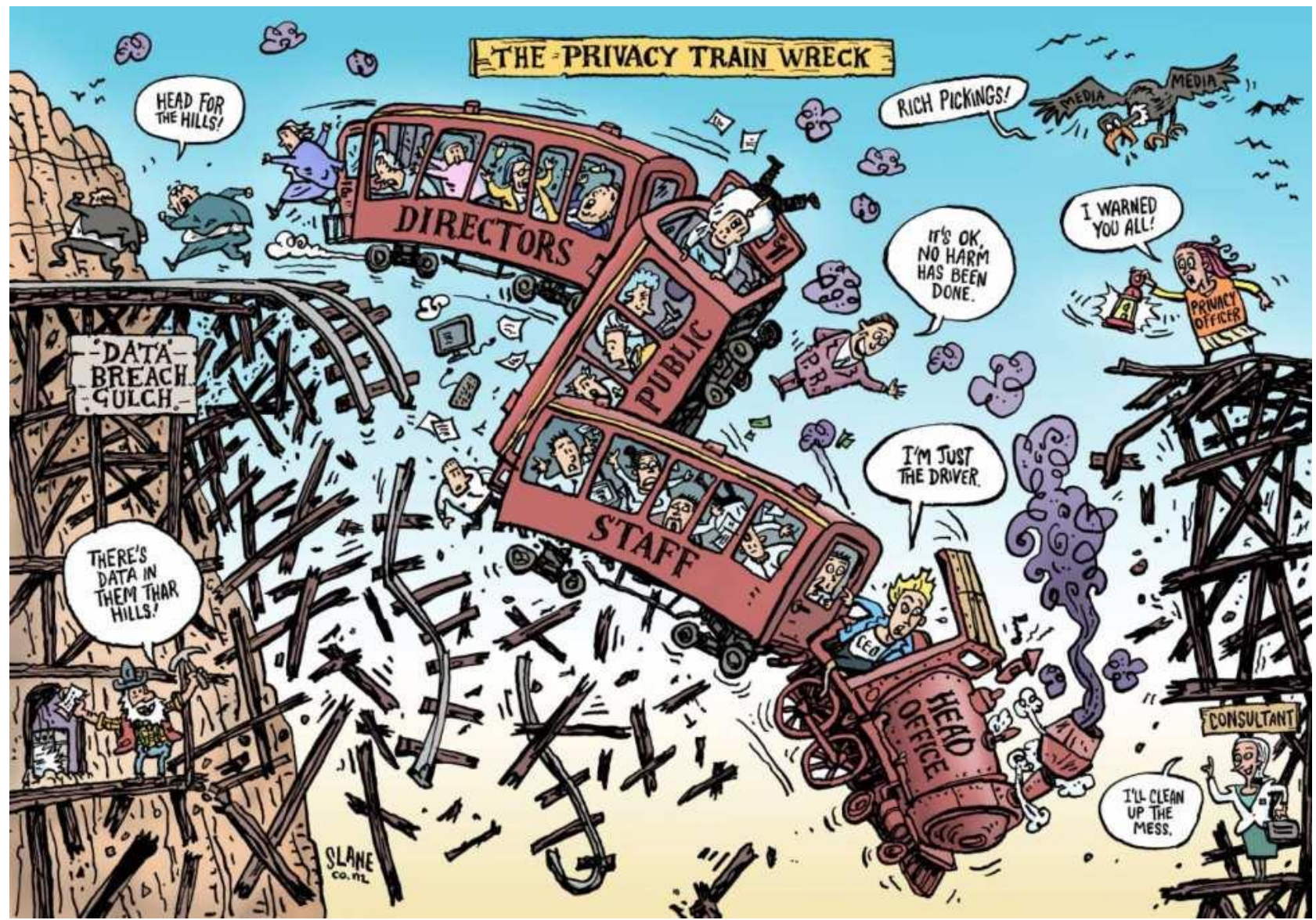
Micro-Enterprises	Small Enterprises	Medium-sized Enterprises	Large Enterprises
Annual turnover less than EUR 2 million	Annual turnover between EUR 2 and 10 million	Annual turnover between EUR 10 and 50 million	Annual turnover more than EUR 50 million
Subgroup 1	Subgroup 1	Subgroup 1	Subgroup 1
Subgroup 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:



Штрафы - интересные кейсы





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 Proteção 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).

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

 Artikel drucken



Bild: SN/FOTOLIA

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.



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

   1041

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.



AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

Seguici su 

Cerca

CHI SIAMO COMPETENZE AUTORITA' 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 l'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 preselezione del più ampio consenso alla condivisione di dati. La decisione dell'utente di limitare il proprio consenso comporta, infatti, la prospettiva di rilevanti limitazioni alla fruibilità del social network e dei siti web/app di terzi; ciò condizionando 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 deselezionare 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

Кто: L'Autorità Garante della Concorrenza e del Mercato – Управление по защите конкуренции и рынка (Италия)

Кого: Facebook Ireland Ltd. и ее материнская компания Facebook Inc.

Когда: 2018.12

За что: нарушение ст. 21 и 22 Codice del Consumo (Кодекса потребителей)

Как: 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 1st 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.


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 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 lovhjemplene 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

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.



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

Infolinia Urzędu 606-950-000

Urząd Ochrony Danych Osobowych 

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 cięższym na nim obowiązku informacyjnym. Sąd decyzyjnie o nałożeniu na ten podmiot kary w tej wysokości - podkreśliła Prezes UODO dr Edyta Bielak-Jomaa

Bardzo wiele osób, których dane przetwarzała 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 mogły 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 12 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 klauzulę informacyjną.

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/номераами телефонов и посчитала слишком дорогостоящим использование таких каналов коммуникации.


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 Stalf. FOTO: WOLFGANG KUMM/DPA

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».



edpb European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

European Data Protection Board > News > National News > National News > First Belgian GDPR fine

First Belgian GDPR fine

Tuesday, 28 May, 2019 BE

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, l'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 électorale 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 électorale 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 peuvent 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 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 proteja drepturile persoanelor vizate. Aceasta a condus la dezvăluirea 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 plăttorului (pentru situațiile în care plăttorul efectua tranzacția dintr-un cont deschis la o altă instituție de credit - tranzacții externe și depuneri la casierie), respectiv a datelor privind adresa plăttorului (pentru situațiile în care plăttorul 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 sesizări 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 dezvăluite 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 prelucreează 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.

Regulament (UE) 2016/679 aplicabil din 25 mai 2018

Plângeri
Plângeri RGPD
Procedura de soluționare

Operatori
Formular de declarație responsabil cu protecția datelor
Notificare Breșă RGPD
Notificare Breșă L.506/2004
Informații plată amendă persoane juridice

Informații utile
Întrebări frecvente
Ghid întrebări RGPD
Ghid orientativ RGPD
Leqături utile

Stiri
08/07/2019
O nouă amendă în aplicarea GDPR
04/07/2019
Prima amendă în aplicarea RGPD

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.

**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.

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 сотрудников. До этого CNIL дважды предупреждала компанию о том, что сотрудники не должны быть постоянными объектами видеосъемки и что им должна быть предоставлена исчерпывающая информация о функционале и целях использования внутренней системы видеонаблюдения.

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 причинённый ущерб согласно ст.82 GDPR.



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.



 **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 сотрудников 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.



РЕПУБЛИКА БЪЛГАРИЯ

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ



Начало
Институцията
Правна рамка
Насоки
Практика
Контакти

Полезна информация

Длъжностно лице по защита на данните

Подаване на жалби и сигнали

Международно сътрудничество

Шенгенско пространство

Анкета

ПРАКТИЧЕСКИ ВЪПРОСИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ СЛЕД 25 МАЙ 2018 Г.

10 ПРАКТИЧЕСКИ СЪПЪКИ ЗА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ДАННИТЕ

ПРАВА НА ФИЗИЧЕСКИТЕ ЛИЦА СЪГЛАСНО РЕГЛАМЕНТ (ЕС) 2018/679, GDPR

Информационни картици



Начало » Информация за извършена проверка в Националната агенция за приходите

Информация за извършена проверка в Националната агенция за приходите

29.08.2019

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 приложила подходящи технически и организационни мерки, в резултат на което е осъществен неотризиран достъп, неразрешено разкриване и разпространение на следните категории лични данни на физически лица: имена, ЕГН и адреси на български граждани, телефони, електронни адреси и друга информация за контакт, данни от годишни данъчни декларации на физически лица, данни от осигурителни декларации, данни за здравноосигурителни вноски (но не и за медицински статус или информация за лечение на гражданите), данни за издадени актове за административни нарушения, данни за извършени плащания на данъци и осигурителни задължения през „Български пощи“ АД, както и данни за поискан и възстановен ДДС, платен в чужбина.

Установено е, че в неправомерно достъпната и разпространена в интернет пространството информация се съдържат лични данни на общо 6 074 140 физически лица, което включва 4 104 786 живи физически лица, български и чужди граждани, и 1 959 598 починали физически лица.

С Решение от 23.08.2019 г. КЗЛД издаде Разпореждания на НАП на основание чл. 58, § 2, буква „г“ във връзка с чл. 57, § 1, буква „а“ и чл. 83, § 2, букви „а“, „в“, „г“, „в“ и „ж“ от Регламент (ЕС) 2016/679 за предприемане на подходящи технически и организационни мерки в контекста на действащото законодателство за защита на личните данни, като напр.:

- мерки с цел повишаване защитата при обработка на лични данни в приложения за електронни услуги към гражданите;
- извършване на анализ на риска на системите и операциите по обработването, включващи изготвени правила и функционални задължения за работа на всяка информационна система;
- извършване на оценка на въздействието при идентифициран „висок риск“ за всяка една система и предприетите мерки;
- извършване на оценка на въздействието при първоначално стартиране на нови информационни системи и приложения.

Срокът за изпълнение на разпорежданията е шестмесечен, считано от датата на получаването им.

На 28.08.2019 г., на основание чл. 87, ал. 3 от Закона за защита на личните данни, Венцислав Караджов - Председател на Комисията за защита на личните данни, издаде Наказателно постановление на НАП за нарушение на чл. 32, § 1, буква „б“ от Регламент (ЕС) 2016/679, с оглед осъществяване неотризиран достъп, неразрешено разкриване и разпространение на личните данни на физически лица от информационните бази данни, поддържани от агенцията. Размерът на наложената санкция е 5 100 000 лева.

тарсене

Политика за поверителност

Годишни отчети

Информационен бюлетин

Профил на купувача

Административно обслужване

Медии

Съобщения

Информационна кампания

По жалби

Кариери

Търгове

Календар на събитията

Септември 2019

п	в	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

Конференция 2015

Конкурс за два

Наредба № 1 от 30 януари 2013 – отменена, считано от 25.05.2018

Въпроси по приложението на ЗЗЛД - архив към 24.05.2018

Въпроси, свързани с провеждането на избори - архив към 24.05.2018

Кто: Комисия за защита на личните данни (Болгария)

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 и организационных мер по защите персональных 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.





[OM OSS](#) [KONTAKTA OSS](#) [PRESS](#) [A-Ö](#) [IN ENGLISH](#)

Sök frågor och svar, vägledning och regler...

[AKTUELLT](#) [VÄGLEDNINGAR](#) [LAGAR OCH REGLER](#) [UTBILDNINGAR OCH KONFERENSER](#)

[Start](#) → [Nyheter](#) → [Sanktionsavgift för ansiktsgenkänning i skola](#)

Publicerad 2019-08-21

Sanktionsavgift för ansiktsgenkänning i skola

Datainspektionen utfärdar en sanktionsavgift på 200 000 kronor för en skola som på prov har använt ansiktsgenkänning via kamera för att registrera elevernas närvaro.

För första gången utfärdar nu Datainspektionen en sanktionsavgift mot en aktör som har brutit mot reglerna i dataskyddsförordningen, GDPR.

En gymnasieskola i Skellefteå har på prov använt ansiktsgenkänning via kamera för att registrera elevernas närvaro på lektionerna. Försöket har pågått under tre veckor och berört 22 elever. Datainspektionen har granskat användningen och konstaterar att gymnasienämnden i Skellefteå har hanterat känsliga personuppgifter i strid med dataskyddsförordningen.

– Gymnasienämnden i Skellefteå har överträtt flera av bestämmelserna i dataskyddsförordningen på ett sätt som gör att vi nu utfärdar en sanktionsavgift, säger Lena Lindgren Schelin, generaldirektör för Datainspektionen.

Sanktionsavgiften är 200 000 kronor. Avgiftens storlek påverkas bland annat av att det är frågan om en myndighet och att det handlar om ett försök under en begränsad period. Myndigheter kan maximalt få tio miljoner kronor i sanktionsavgift.

Кто: Datainspektionen (Швеция)

Кого: школа в городе Скеллефтео

Когда: 2019.08

За что: нарушение ст. 5(1)(c), 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 сотрудников ложное впечатление, что она обрабатывает их персональные данные на законном основании согласия, хотя для такой обработки у компании были иные законные основания.



Urząd
Ochrony
Danych
Osobowych

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 jakiego 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.



edpb European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

National News Administrative fines imposed on a telephone service provider

Administrative fines imposed on a telephone service provider

Monday, 7 October, 2019 GR

Administrative fines imposed on a telephone service provider

(1) Imposition of a fine for breach of the principle of accuracy and data protection by design when keeping personal data of subscribers

The Hellenic DPA has received complaints from telephone subscribers of the Hellenic Telecommunications Organization ("OTE") who, although registered in the OTE's do-not-call register (according to Article 11 of [Law 3471/2006](#)), they received unsolicited calls from third companies for the promotion of products and services.

The investigation of the case showed that those subscribers had submitted a portability request for the transfer of their subscription to another provider. As a consequence, OTE deleted their entries from the do-not-call register. However, when those subscribers cancelled their portability request, there was no proper procedure to cancel their removal from the register. Subscribers were listed as registrants in the internal system of the provider's customer service, but their telephone numbers were not included in the register sent by OTE to the advertisers, as the two systems, due to the error in their interconnection, did not have the same content.

The Authority found that this incident affected a large number of individual subscribers, as there was an infringement of Article 25 (data protection by design) and Article 5 (1) (c) (principle of accuracy) of the General Data Protection Regulation (GDPR). It therefore imposed an administrative fine of EUR 200.000 on the basis of the criteria laid down in Article 83 (2) of the Regulation.

Decision 31/2019 is available in Greek on [www.dpa.gr](#). "Decisions"

(2) Imposition of a fine for failure to satisfy the right to object and the principle of data protection by design when keeping personal data of subscribers

The Hellenic DPA has received complaints from the recipients of advertising messages from OTE concerning their lack of ability to unsubscribe from the list of recipients of advertising messages. In the course of the examination of the complaints it emerged that from 2013 onwards, due to a technical error, the removal from the lists of recipients of advertising messages did not operate for those recipients who used the "unsubscribe" link. OTE did not have the appropriate organisational measure, i.e. a defined procedure by which it could detect that the data subject's right to object could not be satisfied.

Subsequently, OTE removed around 8.000 persons from the addressees of the messages, who had unsuccessfully attempted to withdraw from 2013 onwards. The Authority has found an infringement of the right to object to the processing for direct marketing purposes (Article 21 (3) of the GDPR) as well as Article 25 (data protection by design) of the GDPR and imposed an administrative fine of EUR 200.000 on the basis of the criteria of Article 83 (2) of the Regulation.

Decision 34/2019 is available in Greek on [www.dpa.gr](#). "Decisions"

Communications Department

For further information, please contact the Greek SA directly: contact@dpa.gr

Кто: Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

Кого: Hellenic Telecommunications Organization (OTE)

Когда: 2019.10

За что: нарушение ст. 5(1)(с), 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.



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 причиненный ущерб ему согласно ст.82 GDPR по причине обработки персональных данных без надлежащего правового основания.

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/>

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 22:18 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 cuantum 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 cuantum de 20.000 Euro.

În ceea ce privește **Raiffeisen Bank S.A.**, Autoritatea Națională de Supraveghere a demarat o investigație, ca 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 ANIAF.

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 **ca 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 îi revine în temeiul 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 informatică 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 autorității de supraveghere încălcarea securității datelor cu caracter personal, fără întârzieri nejustificate, 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 vizate) și la prelucrarea neautorizată/ilegală a datelor cu caracter personal ale acestora.

Direcția juridică și comunicare
A.N.S.P.D.C.P.

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.



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

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 ασθενοείας των εργοδοτούμενων 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 λήγει 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. Αναφ.: Ε/ΜΜ/Company-89/6 και με ημερομηνία 02.09.2019, με την οποία παραθέσατε τις εισηγήσεις των πελατών σας και σας πληροφορώ τα ακόλουθα:

Γενονότα

1.1. Στις 06.06.2018, δέχτηκα 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 εργοδοτούμενων για λόγους ασθενοείας, χρησιμοποιώντας ένα εργαλείο βαθμολόγησης, γνωστό ως «ο Συντελεστής Bradford» (Bradford Factor). Το εν λόγω σύστημα είναι επίσης προσβάσιμο στο ενδο-διαδίκτυο 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 διαφώνια του για τη λειτουργία του εν λόγω συστήματος και τον προειδοποίησε 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 προέτρεψε/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 Αυτών (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 εργοδοτούμενοι παρουσιάζουν συστηματικά από την εργασία τους λόγω ασθενοείας.

Ανέφεραν ότι, αντιμετωπίζουν ιδιαίτερο πρόβλημα στο αεροδρόμιο Λάρνακας, όπου λόγω της φύσης της εργασίας (εργασία με σύστημα βάρδιας), αρκετοί εργοδοτούμενοι, ιδιαίτερα τα Σαββατοκύριακα, απουσιάζουν συστηματικά από την εργασία τους και παρουσιάζουν άδεια ασθενοείας.

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.



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

Friday, 11 October, 2019 NO

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

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.



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, 6 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: kancelaria@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.



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

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.



EDPS
EUROPEAN DATA PROTECTION SUPERVISOR
The EU's independent data protection authority

Home About Data Protection Press & Publications

Home > ... > 2019 > EDPS investigates European Parliament's 2019 election activities and takes enforcement actions

EDPS investigates European Parliament's 2019 election activities and takes enforcement actions

28 Nov 2019

EDPS investigates European Parliament's 2019 election activities and takes enforcement actions [Press Release](#)

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.

Wojciech Wiewiórowski, Assistant EDPS, said: *"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."*

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 голосованию на весенних выборах 2019 года, которая проводилась посредством веб-сайта thistimeimvoting.eu и привела к обработке данных более чем 329,000 человек. Первый выговор был вызван неосведомлённостью 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.



The screenshot shows the website of the Hungarian Competition Authority (GVH). The main navigation bar includes 'GVH', 'FOR PROFESSIONAL USERS', and 'PRESS ROOM'. The 'PRESS ROOM' section is active, displaying a list of press releases from 2005 to 2019. The selected release is titled 'GVH imposed a fine of EUR 3.6 M on Facebook'. The content of the release states that the GVH found Facebook Ireland Ltd. in violation of competition law for advertising its services as free of charge on its homepage and Help Centre. The fine of EUR 3.6 million is the highest ever imposed by the Authority in a consumer protection case. The release also discusses the 'zero price' model of Facebook, which attracts users by offering free services while collecting and using their data for targeted advertising. The GVH found that Facebook's slogans were deceptive and that the company did not fully disclose the risks and obligations associated with its services.

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.



BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

DATENSCHUTZ | INFORMATIONSFREIHEIT | **INFOTHEK** | BFDI | ZENTRALE ANL

→ Infothek → Pressemitteilungen → BfDI verhängt Geldbußen gegen Telekommunikationsdie

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.



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 /

London pharmacy fined after “careless” storage of patient data

Date 20 December 2019
Type News

The Information Commissioner's Office (ICO) has fined a London-based pharmacy £275,000 for failing to ensure the security of special category data.

Doorstep Dispensaree Ltd, which supplies medicines to customers and care homes, left approximately 500,000 documents in unlocked containers at the back of its premises in Edgware. The documents included names, addresses, dates of birth, NHS numbers, medical information and prescriptions belonging to an unknown number of people.

Documents, some of which had not been appropriately protected against the elements and were therefore water damaged, were dated between June 2016 and June 2018. Failing to process data in a manner that ensures appropriate security against unauthorised or unlawful processing and accidental loss, destruction or damage is an infringement of the General Data Protection Regulation (GDPR).

The ICO launched its investigation into Doorstep Dispensaree after it was alerted to the insecurely stored documents by the Medicines and Healthcare Products Regulatory Agency, which was carrying out its own separate enquiry into the pharmacy.

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).



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 tásor 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.



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

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 (Egl), totalling 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 Egl.

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 Egl and highlighted serious criticalities 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 Egl 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. Egl 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 Egl.

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 Egl 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 Egl 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 Egl 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.



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 SpA

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).

Associated Press
EuroWeekly

THE Spanish Agency for Data Protection (AEPD) has handed out a penalty of €10,000 for sharing intimate photos and screenshots of a woman's conversations in WhatsApp without her consent.

The fine is the first of its kind in Spain and somewhat of a controversial decision as has made an example of the man's behaviour, which although was illicit, is perceived by a proportion of the population as innocent.

The Agency's decision now opens the doors to apply the European Data Protection Regulation (GDPR) directly on citizens, which according to privacy experts, is usually intended to be applied to companies and one which provides a stark warning to others.

The victim had reported to the AEPD in July 2019 that her privacy had been breached after several people told her that they had seen intimate photographs and screenshots of conversations on WhatsApp between herself and a co-worker. The images were also accompanied by hurtful and vexatious comments.

A fine was issued as according to the AEPD, sharing personal data from third parties without their consent constitutes a "very serious infraction." Detailing the penalty, the Agency indicated that although there is no record that the sanctioned man expressly wanted to violate the right to data protection of the victim, the comments attached to the photographs show a "serious negligence." They had also lowered the penalty as the sharing of the content was one of a "purely local" scope and that only one person was affected.

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.

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
 ✉ 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 не 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.



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.



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 Gdańska. 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 uprawnienia dziecka do odebrania obiady. 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 uprawnienia dziecka do odebrania obiady.



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.



Datainspektionen OM OSS KONTAKTA OSS PRESS A-Ö IN ENGLISH

Sök frågor och svar, vägledning och regler...

AKTUELLT VÄGLEDNINGAR LAGAR OCH REGLER UTBILDNINGAR OCH KONFERENSER

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.



The screenshot shows the website of the European Data Protection Board (EDPB). The main navigation bar includes 'HOME', 'ABOUT EDPB', 'NEWS', and 'OUR WORK & TOOLS'. The article title is 'Fine imposed for preventing the Supervisory Authority from performing an inspection'. The date is 'Friday, 3 April, 2020'. The article text describes a fine of PLN 20,000 imposed on Vis Consulting Sp. z o.o. for preventing the supervisory authority from performing an inspection. The text mentions that the company's owner is subject to criminal liability for this. It also states that the UODO decided to conduct inspection activities at the penalised company, in connection with the findings made in the course of another inspection performed at the company conducting telemarketing activities. It was established that the company has a cooperation contract with regard to outsourcing of telemarketing services with Vis Consulting Sp. z o.o. Therefore, the supervisory authority found it necessary to conduct inspection activities at the entity which actually operated the telephone calls and processed the data. Unfortunately, the UODO's inspectors, after prior notification on the planned inspection, did not find anyone at the address indicated in the National Court Register (KRS). On the spot, there was only a company which leased office space to Vis Consulting Sp. z o.o. (so called virtual office). The inspectors managed, however, to contact Vis Consulting by telephone, and its proxy informed that the inspection would not take place. Therefore, the President of the UODO concluded that the company in no way wished to cooperate with the personal data protection authority. On two consecutive days of the planned inspection activities, the company made it impossible to carry out the inspection twice. Furthermore, on the date on which the inspectors attempted to conduct inspection at Vis Consulting Sp. z o.o., its authorities decided to liquidate that entity. In the opinion of the President of the Office, this company does not comply with the obligations relating to the processing of personal data and, at least intentionally, avoids to be subject of inspection by the supervisory authority. Thus the company infringed the provisions of Article 31 of the GDPR with regard to Article 58(1)(e) and (f) of the GDPR referring to cooperation with the supervisory authority and enabling it access to all personal data and any information. Hence, the President of the UODO concluded that the conditions for imposing a fine on the company were satisfied. In determining the amount of the fine, the supervisory authority did not identify any attenuating circumstances affecting the amount of the fine. In connection with suspicion of commission of an offence under Article 108 (1) of the Act on the Protection of Personal Data by the President of the Company, the supervisory authority notified the District Public Prosecutor's Office in Katowice thereof. According to that provision, the prevention or hindering of conducting inspection of compliance with the personal data protection provisions shall be subject to a fine, restriction of personal liberty or imprisonment for up to two years. The Public Prosecutor's Office has already lodged an indictment against the President of the Company to the court.

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.



**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 сотрудников 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 сотрудники зависят от своего работодателя, поэтому их согласие на использование подобной системы не может быть оценено как свободное.



edpo YOUR EU REPRESENTATIVE

HOME SERVICES ABOUT PRICING CERTIFICATE

DPO and conflict of interest: the Belgian DPA issues a 50,000 EUR fine

On 28 April 2020, the Belgian Data Protection Authority ("DPA"), fined a Belgian company 50,000 EUR for breach of article 38 (6) of the GDPR. The DPA's Litigation Chamber found that the DPO was not in a position that is sufficiently free from conflict of interest because the DPO also fulfilled the function of director of audit, risk and compliance.

The Litigation Chamber stated that the administrative fine was not imposed with the intention to terminate the violation, but rather with a view to vigorously enforce the rules of the GDPR. In this respect, the Litigation Chamber specified that, although there was no element showing an intentional infringement, there was serious negligence on the part of the defendant. Please find below a non-official English translation of the excerpt of the decision which covers the DPO conflict of interest.

Follow this link to read the full version of the DPA's decision (available only in Dutch): <https://lnkd.in/dNXzrUt>

NON-OFFICIAL ENGLISH TRANSLATION

Decision of the Belgian Data Protection Authority of 28 April 2020 :

DPO conflict of interest

Кто: l'Autorité de protection des données (Бельгия)

Кого: Proximus SA


Когда: 2020.04

За что: нарушение ст. 32 и 38(6) GDPR

Как: штраф €50,000

Причина: утечка персональных данных, а также нарушения порядка взаимодействия с регулятором, неисполнение принципа подотчетности (accountability), невыполнение риск-ориентированного подхода при защите данных, наличие конфликта интересов у DPO, недостаточное вовлечение DPO в разрешение вопросов по обработке и защите персональных данных в компании. Большая часть нарушений была снята в результате судебного слушания по жалобе контролера. При расчете штрафа также была учтена длительность нарушения (2 года).





[OM OSS](#) [KONTAKTA OSS](#) [PRESS](#) [A-Ö](#) [IN ENGLISH](#)

Sök frågor och svar, vägledning och regler...

[AKTUELLT](#) [VÄGLEDNINGAR](#) [LAGAR OCH REGLER](#) [UTBILDNINGAR OCH KONFERENSER](#)

[Start](#) → [Nyheter](#) → [Fel publicera känsliga personuppgifter på Region Örebro läns webb](#)

Publicerad 2020-05-12

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.



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)

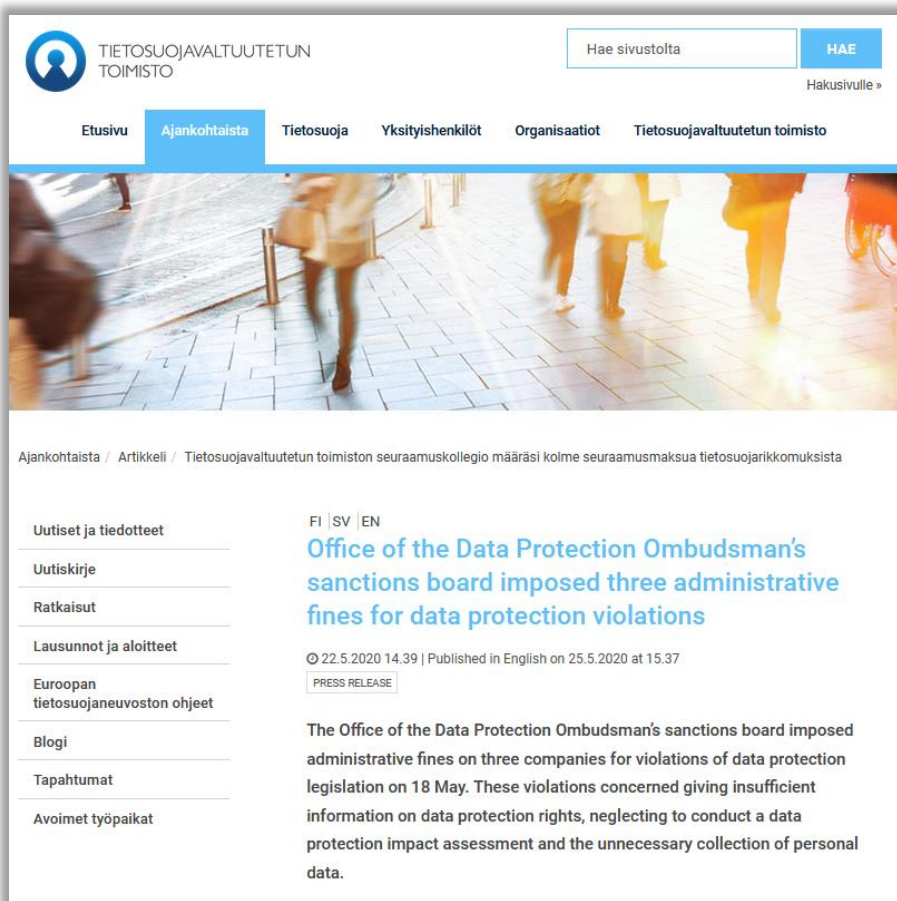
Кого: JobTeam

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.



TIETOSUOJAVALTUUTETUN TOIMISTO

Hae sivustolta HAE Hakusivulle »

Etusivu Ajankohtaista Tietosuoja Yksityishenkilöt Organisaatiot Tietosuojavaaltuutetun toimisto

Ajankohtaista / Artikkelit / Tietosuojavaaltuutetun toimiston seuraamuskollegio määräsi kolme seuraamusmaksua tietosuojarikkomuksista

Uutiset ja tiedotteet

Uutiskirje

Ratkaisut

Lausunnot ja aloitteet

Euroopan tietosuojaneuvoston ohjeet

Blogi

Tapahtumat

Avoimet työpaikat

FI | SV | EN

Office of the Data Protection Ombudsman's sanctions board imposed three administrative fines for data protection violations

© 22.5.2020 14:39 | Published in English on 25.5.2020 at 15:37

PRESS RELEASE

The Office of the Data Protection Ombudsman's sanctions board imposed administrative fines on three companies for violations of data protection legislation on 18 May. These violations concerned giving insufficient information on data protection rights, neglecting to conduct a data protection impact assessment and the unnecessary collection of personal data.

Кто: Tietosuojavaaltuutetun toimisto (Финляндия)

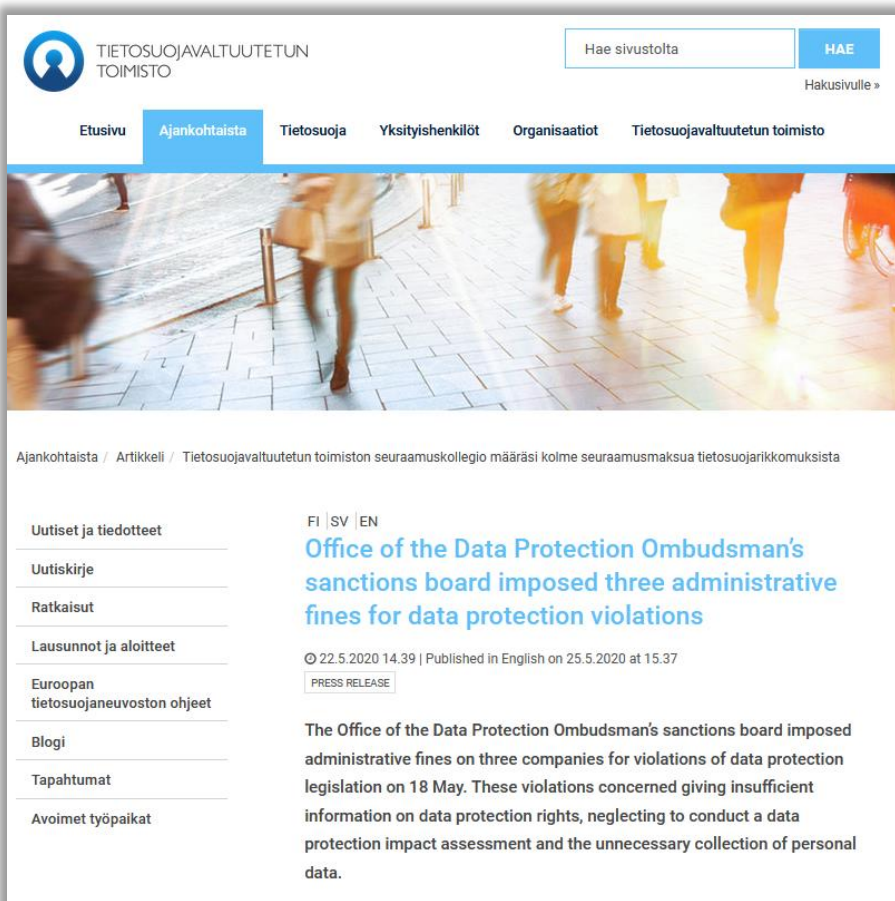
Кого: Posti Oy (Почта Финляндии)

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.



TIETOSUOJAVALTUUTETUN TOIMISTO

Hae sivustolta HAE Hakusivulle »

Etusivu Ajankohtaista Tietosuoja Yksityishenkilöt Organisaatiot Tietosuojavaaltuutetun toimisto

Ajankohtaista / Artikkelit / Tietosuojavaaltuutetun toimiston seuraamuskollegio määräsi kolme seuraamusmaksua tietosuojarikkomuksista

Uutiset ja tiedotteet

Uutiskirje

Ratkaisut

Lausunnot ja aloitteet

Euroopan tietosuojaneuvoston ohjeet

Blogi

Tapahtumat

Avoimet työpaikat

FI | SV | EN

Office of the Data Protection Ombudsman's sanctions board imposed three administrative fines for data protection violations

© 22.5.2020 14:39 | Published in English on 25.5.2020 at 15:37

PRESS RELEASE

The Office of the Data Protection Ombudsman's sanctions board imposed administrative fines on three companies for violations of data protection legislation on 18 May. These violations concerned giving insufficient information on data protection rights, neglecting to conduct a data protection impact assessment and the unnecessary collection of personal data.

Кто: Tietosuojavaaltuutetun toimisto (Финляндия)

Кого: Kymen Vesi Oy

Когда: 2020.05

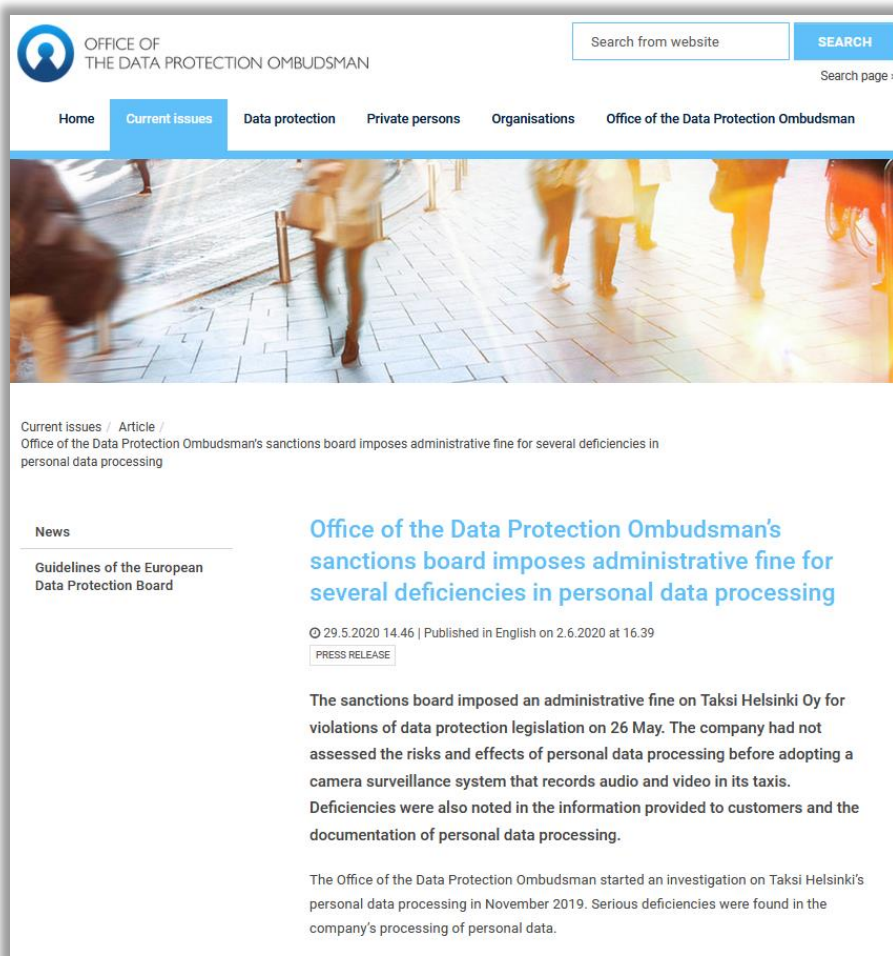
За что: нарушение ст.35 GDPR

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.



OFFICE OF THE DATA PROTECTION OMBUDSMAN

Search from website

Search page »

Home **Current issues** Data protection Private persons Organisations Office of the Data Protection Ombudsman

Current issues / Article / Office of the Data Protection Ombudsman's sanctions board imposes administrative fine for several deficiencies in personal data processing

News

Guidelines of the European Data Protection Board

Office of the Data Protection Ombudsman's sanctions board imposes administrative fine for several deficiencies in personal data processing

© 29.5.2020 14.46 | Published in English on 2.6.2020 at 16.39

PRESS RELEASE

The sanctions board imposed an administrative fine on Taksi Helsinki Oy for violations of data protection legislation on 26 May. The company had not assessed the risks and effects of personal data processing before adopting a camera surveillance system that records audio and video in its taxis. Deficiencies were also noted in the information provided to customers and the documentation of personal data processing.

The Office of the Data Protection Ombudsman started an investigation on Taksi Helsinki's personal data processing in November 2019. Serious deficiencies were found in the company's processing of personal data.

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.



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.

- Procedimiento Nº: PS/00417/2019

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: A.A.A., y B.B.B. (en adelante, los reclamantes) con fecha 21 de mayo y 4 de noviembre de 2019 respectivamente interpusieron reclamación ante la Agencia Española de Protección de Datos.

Sus reclamaciones se dirigen contra **GLOVOAPP23, S.L.** con NIF **B66362906** (en adelante, el reclamado).

Los motivos en que basan su reclamación son que no tienen nombrado un Delegado de Protección de Datos (en adelante DPD) al que dirigir las reclamaciones.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 2 de julio de 2019, la primera reclamación fue trasladada a la reclamada la reclamación presentada para su análisis y comunicación al reclamante de la decisión adoptada al respecto.

La reclamada contesta al traslado de la reclamación afirmando que no se encuentran ni entre los supuestos del art. 37 RGPD ni el del 34 LOPGDD, con lo que no tienen obligación de designar un DPD.

TERCERO: Con fecha 13 de enero de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del artículo 37 del RGPD, tipificada en el artículo 83.4 del RGPD.

CUARTO: Notificado el 22 de enero de 2020 el citado acuerdo de inicio, el reclamado presentó el 31 de enero de 2020 escrito de alegaciones en el que, en síntesis, manifestaba que su actividad de tratamiento de datos personales se encuentra exenta de las obligaciones establecidas en los artículos 37 RGPD y 34 LOPGDD, y, por tanto, exenta de la obligación de designar un Delegado de Protección de Datos.

Sin embargo, alega que en ningún momento ha negado la existencia de un órgano que se dedicara, en el contexto de la organización, al desempeño de las funciones que son propias de un Delegado de Protección de Datos, ya que el 8 de junio de 2018, constituyó el Comité de Protección de Datos, con el fin de cubrir los ámbitos técnicos de la empresa y en la misma fecha, se designó también un Subcomité de Protección de Datos, a fin de dar cumplimiento a la autorización del Consejo de Administración de constituir dicho comité.

Concluye afirmando que el Comité de Protección de Datos, lleva a cabo las funciones propias de un Delegado de Protección de Datos descritas en el artículo 39 del RGPD.

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.

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, (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, (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.
Ci0	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
sedeagpd.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.



**AUTORITEIT
PERSOONSgegevens**

Home Corona Over privacy ▾ Onderwerpen ▾ Zelf doen ▾

Boete voor BKR vanwege kosten bij inzage persoonsgegevens

Nieuwsbericht / 6 juli 2020

Categorie:
[Recht op inzage,](#)
[Rechten van betrokkenen,](#)
[Krediet, inkomen en faillissement](#)

Stichting Bureau Krediet Registratie (BKR) mag geen geld vragen aan mensen die digitaal hun persoonsgegevens willen inzien. En wanneer mensen per post inzage in hun persoonsgegevens bij BKR willen, moet dat eenvoudig en met redelijke tussenpozen mogelijk zijn. BKR wierp te hoge drempels op voor inzage. Dat mag niet volgens de privacywetgeving. Daarom heeft de Autoriteit Persoonsgegevens (AP) BKR een boete opgelegd van 830.000 euro. De AP kreeg klachten over de drempels die BKR opwierp wanneer mensen hun persoonsgegevens wilden inzien. Dit was voor de AP aanleiding om onderzoek te doen.

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



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Operatori telefonici: continua l'attività di controllo del Garante privacy, sanzione a Wind per 17 milioni di euro e a Iliad per 800 mila euro

Operatori telefonici: continua l'attività di controllo del Garante privacy, sanzione a Wind per 17 milioni di euro e a Iliad per 800 mila euro

Continua l'attività di controllo del Garante per la protezione dei dati personali nei confronti degli operatori telefonici anche a seguito delle centinaia di segnalazioni e reclami che settimanalmente pervengono all'Autorità per lamentare casi di "marketing selvaggio".

Nell'ambito di tali attività di controllo, nella riunione del 9 luglio scorso, l'Autorità ha sanzionato Wind Tre Spa per circa 17 milioni di euro per numerosi trattamenti illeciti di dati, legati prevalentemente ad attività promozionali. Per analoghe violazioni, la società era già stata destinataria di un provvedimento inibitorio e prescrittivo quando era ancora in vigore il vecchio Codice privacy.

Il nuovo provvedimento è stato adottato all'esito di una complessa attività istruttoria ed ispettiva. Gli utenti lamentavano la ricezione di contatti promozionali indesiderati, effettuati senza consenso tramite sms, e-mail, fax, telefonate e chiamate automatizzate. In numerosi casi, inoltre i segnalanti dichiaravano di non esser stati messi in grado di poter esercitare il proprio diritto di revoca del consenso o di opposizione al trattamento dei loro dati per finalità di marketing (anche a causa di imprecisioni nell'indicazione dei canali di contatto presenti nell'informativa). In altri casi veniva lamentata la pubblicazione di dati personali negli elenchi telefonici pubblici nonostante l'opposizione (a volte reiterata) degli interessati.

Dall'istruttoria è inoltre emerso che le app MyWind e My3 erano impostate in maniera tale da obbligare l'utente a fornire, ad ogni nuovo accesso, una serie di consensi per diverse finalità di trattamento (marketing, profilazione, comunicazione a terzi, arricchimento e geolocalizzazione), salvo poi consentire di revocarli trascorse 24 ore.

Al di là di queste lacune "di sistema", gli accertamenti del Garante hanno messo in luce diversi gravi illeciti nella filiera dei partner commerciali di Wind Tre, anche con impropria attivazione di contratti. Per queste violazioni, uno dei partner del gestore telefonico - che aveva sub affittato (peraltro senza alcun atto giuridico) intere fasi dei trattamenti a call-center che raccoglievano i dati illecitamente - è stato multato per 200mila euro dal Garante e si è visto imporre il divieto di utilizzare i dati raccolti e trattati da agenti presenti sul territorio nazionale (denominati "procacciatori") in totale spregio delle norme in materia di protezione dati.

Le argomentazioni portate a propria difesa da Wind Tre e la serie di misure correttive implementate dalla società, anche riguardo alla centralizzazione delle campagne promozionali, non sono state ritenute adeguate dal Garante. Oltre a sanzionare la società telefonica per 16.729.600 euro, l'Autorità ha vietato a Wind il trattamento dei dati acquisiti senza consenso e le ha ordinato di adottare misure tecniche e organizzative per un effettivo controllo della filiera dei partner, nonché procedure per rispettare la volontà degli utenti di non essere disturbati.

Nel corso della stessa riunione del 9 luglio, il Garante ha preso in esame anche le risultanze degli accertamenti disposti nei confronti di un altro gestore telefonico, Iliad, che è stato trovato carente sotto altri profili, in particolare in merito alle modalità di accesso dei propri dipendenti ai dati di traffico e che per tali ragioni, è stato sanzionato per 800.000 euro.

Roma, 13 luglio 2020

Кто: Garante per la protezione dei dati personali (Италия)

Кого: Wind Tre S.p.A.

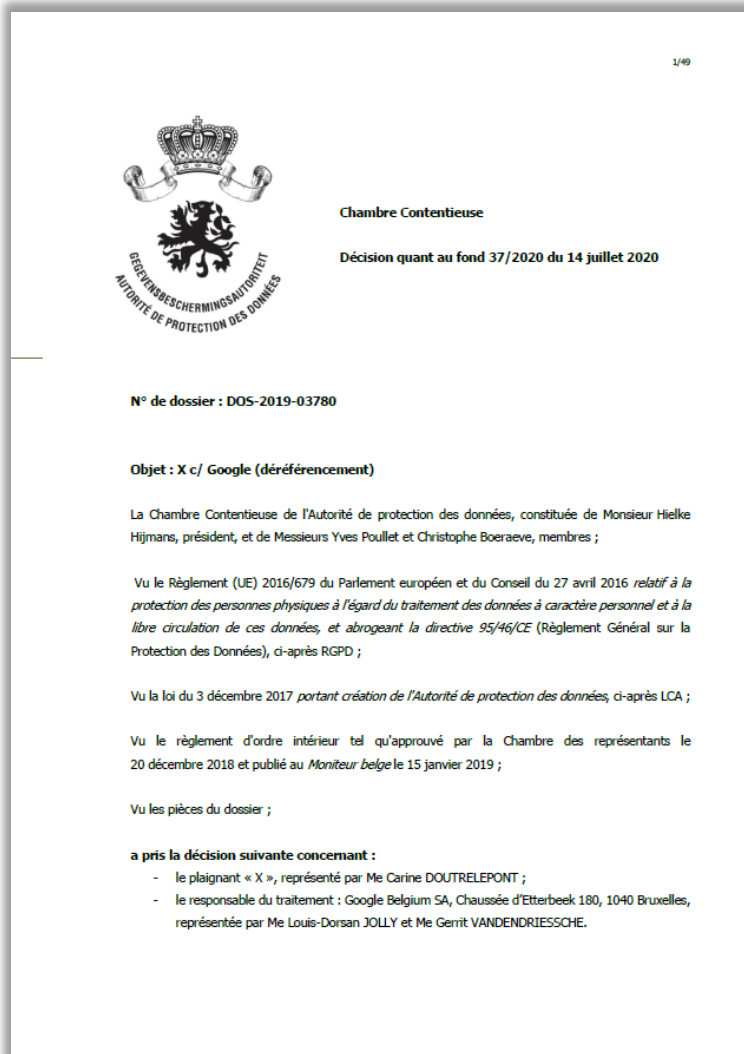
Когда: 2020.07

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.



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.



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 сотрудников и предотвращения мошенничества, CNIL считает, что постоянная запись телефонных разговоров с сотрудниками 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.



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



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 lejerers 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). Регулятор посчитал, что компания не реализовала достаточные организационные и технические меры по защите персональных данных (ТОМs).



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)

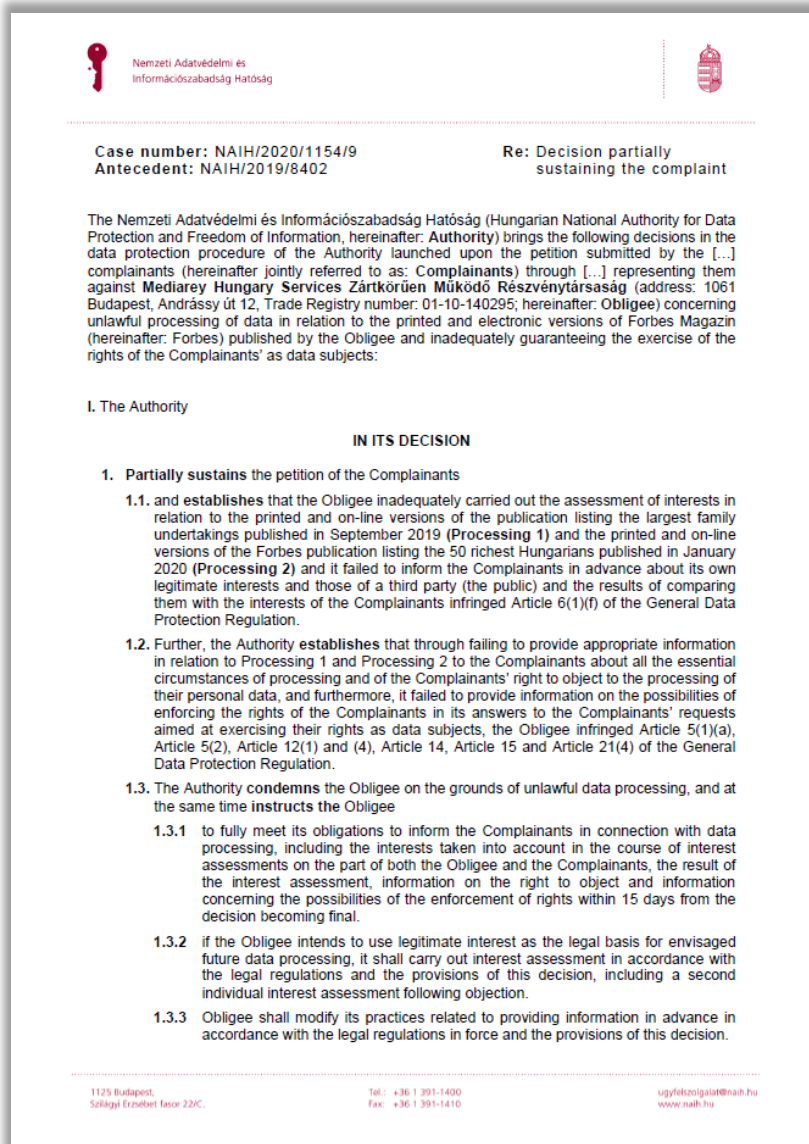
Кого: Statens vegvesen (Государственное управление автомобильных дорог Норвегии)

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 сотрудников. 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.



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.



Hamburg
Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

DATENSCHUTZ ▾ INFORMATIONSFREIHEIT ▾ UNSERE BEHÖRDE ▾ SERVICE UND MEDIENBILDUNG ▾

Bußgeld wegen Datenschutzverstößen bei H&M

35,3 Millionen Euro Bußgeld wegen Datenschutzverstößen im Servicecenter von H&M

01.10.2020 • H&M

Im Fall der Überwachung von mehreren hundert Mitarbeiterinnen und Mitarbeitern des H&M Servicecenters in Nürnberg durch die Center-Leitung hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) einen Bußgeldbescheid in Höhe von 35.258.707,95 Euro gegen die H&M Hennes & Mauritz Online Shop A.B. & Co. KG erlassen.

Die Gesellschaft mit Sitz in Hamburg betreibt ein Servicecenter in Nürnberg. Mindestens seit dem Jahr 2014 kam es bei einem Teil der Beschäftigten zu umfangreichen Erfassungen privater Lebensumstände. Entsprechende Notizen wurden auf einem Netzlaufwerk dauerhaft gespeichert. Nach Urlaubs- und Krankheitsabwesenheiten – auch kurzer Art – führten die vorgesetzten Teamleader einen sogenannten Welcome Back Talk durch. Nach diesen Gesprächen wurden in etlichen Fällen nicht nur konkrete Urlaubsergebnisse der Beschäftigten festgehalten, sondern auch Krankheitssymptome und Diagnosen. Zusätzlich eigneten sich einige Vorgesetzte über Einzel- und Flurgespräche ein breites Wissen über das Privatleben ihrer Mitarbeitenden an, das von eher harmlosen Details bis zu familiären Problemen sowie religiösen Bekenntnissen reichte. Die Erkenntnisse wurden teilweise aufgezeichnet, digital gespeichert und waren mitunter für bis zu 50 weitere Führungskräfte im ganzen Haus lesbar. Die Aufzeichnungen wurden bisweilen mit einem hohen Detailgrad vorgenommen und im zeitlichen Verlauf fortgeschrieben. Die so erhobenen Daten wurden neben einer akribischen Auswertung der individuellen Arbeitsleistung u.a. genutzt, um ein Profil der Beschäftigten für Maßnahmen und Entscheidungen im Arbeitsverhältnis zu erhalten. Die Kombination aus der Ausforschung des Privatlebens und der laufenden Erfassung, welcher Tätigkeit sie jeweils nachgingen, führte zu

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.

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.


GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento su data breach - 1° ottobre 2020 [9469345]

[VEDI ANCHE Newsletter del 26 ottobre 2020](#)

[doc. web n. 9469345]

Provvedimento su data breach - 1° ottobre 2020

Registro dei provvedimenti
n. 174 del 1° ottobre 2020

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 dott. Claudio Filippi, vice 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");

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");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4/4/2019, pubblicato in G.U. n. 108 dell'8/5/2019 e in www.gpdp.it, doc. web n. [9107633](#) (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal vice segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. [1098801](#);

Relatore l'avv. Guido Scorza;

PREMESSO

1. La violazione dei dati personali.

L'Università Campus Bio-medico di Roma (di seguito Campus Bio-medico) ha notificato al Garante una violazione di dati personali ai sensi dell'art. 33 del Regolamento relativamente al "sistema attraverso cui viene fornito al pubblico il servizio di consultazione on line dei referti", a seguito della quale alcuni utenti hanno potuto visualizzare "dati relativi alla salute, in particolare immagini radiologiche associate a dati identificativi e referti clinici" di 74 altri utenti (comunicazione del XX, prot. n. XX).

Secondo quanto notificato, "i dati personali oggetto della violazione sono stati visualizzati da un numero limitato di soggetti determinati (allo stato, non più di 39 utenti), e che tali soggetti, in quanto pazienti/utenti alla stregua degli interessati, si trovano,



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 сотрудникам 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».

Кто: Garante per la protezione dei dati personali (Италия)

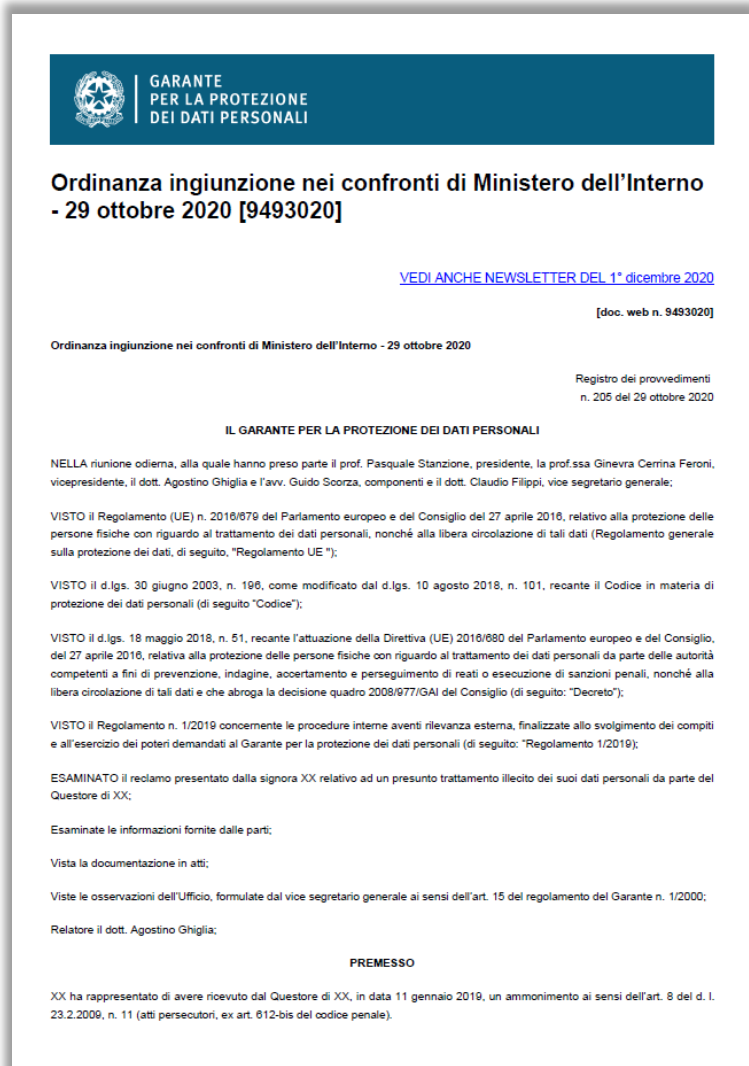
Кого: Министерство внутренних дел Италии


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.



 **GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

**Ordinanza ingiunzione nei confronti di Ministero dell'Interno
- 29 ottobre 2020 [9493020]**

[VEDI ANCHE NEWSLETTER DEL 1° dicembre 2020](#)

[doc. web n. 9493020]

Ordinanza ingiunzione nei confronti di Ministero dell'Interno - 29 ottobre 2020

Registro dei provvedimenti
n. 205 del 29 ottobre 2020

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 dott. Claudio Filippi, vice segretario generale;

VISTO il Regolamento (UE) n. 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 (Regolamento generale sulla protezione dei dati, di seguito, "Regolamento UE");

VISTO il d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, recante il Codice in materia di protezione dei dati personali (di seguito "Codice");

VISTO il d.lgs. 18 maggio 2018, n. 51, recante l'attuazione della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito: "Decreto");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali (di seguito: "Regolamento 1/2019");

ESAMINATO il reclamo presentato dalla signora XX relativo ad un presunto trattamento illecito dei suoi dati personali da parte del Questore di XX;

Esaminate le informazioni fornite dalle parti;


Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal vice segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Agostino Ghiglia;

PREMESSO

XX ha rappresentato di avere ricevuto dal Questore di XX, in data 11 gennaio 2019, un ammonimento ai sensi dell'art. 8 del d. l. 23.2.2009, n. 11 (atti persecutori, ex art. 612-bis del codice penale).



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](#) /
 ICO fines Ticketmaster UK Limited £1.25million for failing to protect customers' payment details

ICO fines Ticketmaster UK Limited £1.25million for failing to protect customers' payment details

Date **13 November 2020**
 Type **News**

The Information Commissioner's Office (ICO) has [fined Ticketmaster UK Limited £1.25million for failing to keep its customers' personal data secure](#).

The ICO found that 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



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 dati personali - composto da Pasquale Stanzone, Ginevra Cerrina Feroni, 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'operatore telefonico 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 sedicenti 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 12.251.001,00 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 contratti siano attivati solo a seguito di chiamate promozionali effettuate dalla sua rete di vendita, attraverso numerazioni censite e iscritte al Roc. Vodafone dovrà anche irrobustire le misure di sicurezza al fine di impedire accessi abusivi ai 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

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.



Datainspektionen OM OSS KONTAKTA OSS PRESS A-Ö IN ENGLISH

Sök frågor och svar, vägledning och regler...

AKTUELLT FRÅGOR OCH SVAR VÄGLEDNINGAR LAGAR OCH REGLER

Start → Nyheter → Sanktionsavgift för olaglig kamerabevakning på LSS-boende

Publicerad 2020-11-25

Sanktionsavgift för olaglig kamerabevakning på LSS-boende

Datainspektionen utfärdar en sanktionsavgift på 200 000 kronor mot Gnosjö kommun med anledning av olaglig kamerabevakning på ett LSS-boende.

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.

– 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.

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 Гноссе

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.

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 и 21 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 и 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 и carrefour-banque.fr несколько файлов cookie, связанных с рекламными активностями, автоматически загружались на пользовательские устройства без получения предварительного согласия пользователей.

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 и 21 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.

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)

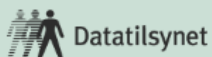
Кого: электронные аптеки Apotheka, Südameapteek и Azeta.ee

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, сотрудник Инспекции по защите данных постели вебсайт электронной аптеки, где он смог получить быстрый доступ к информации о рецептах других лиц с помощью онлайн чата.



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.

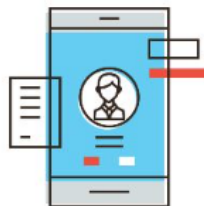
Datatilsynet vurderer at Norges idrettsforbund ikke hadde iverksatt gode nok sikkerhetsrutiner for testingen, og at det ikke var nødvendig å teste med et slikt omfang av personopplysninger.

– 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.



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).

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).

- 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.

Иные санкции и меры принуждения





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 AggregatelQ Data Services Ltd
6 July 2018

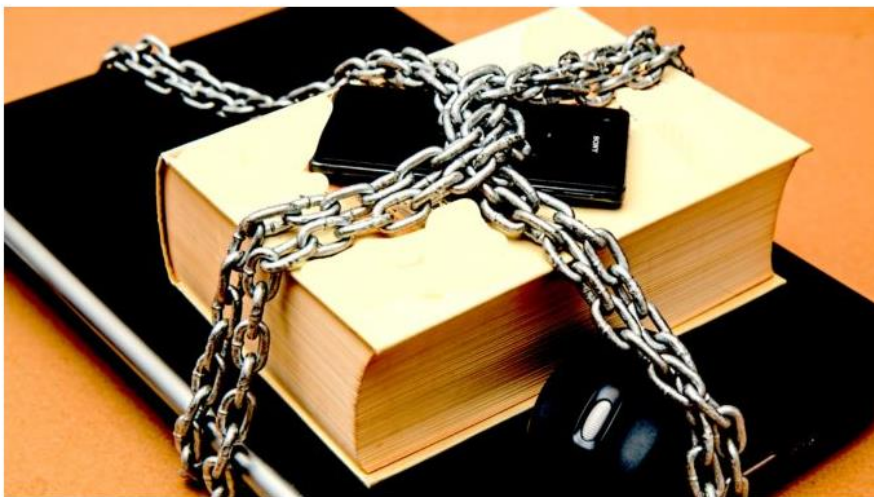
Канадская компания AggregatelQ Data Services, на основании статьи 3(2)(b) GDPR, получила предписание от британского регулятора прекратить обработку любых персональных данных граждан Великобритании или ЕС, полученных от политических организаций Великобритании или иных лиц, для целей аналитики данных, политической агитации или любых других рекламных целей.

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.

Enforcement Notice of the Information Commissioner

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.

The Data Protection Ombudsman ordered Svea Ekonomi to correct its practices in the processing of personal data

Wednesday, 24 April, 2019 

Two cases concerning Svea Ekonomi, a financial credit company, have been processed at the Office of the Data Protection Ombudsman. As a result, the Data Protection Ombudsman has 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.

One of the cases concerning Svea Ekonomi has been processed at the Office of the Data Protection Ombudsman as a complaint made by a single data subject. It concerned the personal data used to assess creditworthiness and the data subject's right to inspect data concerning them. Furthermore, the Office of the Data Protection Ombudsman began to process the matter concerning the company's notification practices upon its own initiative.

In its decision, the Data Protection Ombudsman stated 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 Data Protection 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 Data Protection 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 Data Protection 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 Data Protection 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](mailto:reijo.aarnio(at)om.fi)

Tietosuojavaltuutetun 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.



The screenshot shows a news article on the EDPB website. The article title is "Temporary suspension of the Norwegian Covid-19 contact tracing app". The date is "Monday, 22 June, 2020" with a "NO" tag. The text discusses the Norwegian Data Protection Authority's decision to suspend the Smittestopp app. It mentions that the app collects large quantities of personal data, including location data and contact information. The article also notes that the suspension is temporary and that the app will be re-evaluated once the pandemic situation improves.

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.

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.



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. 196, 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 svoltosi 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:



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.).


Судебная практика – базы решений и интересные ситуации



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



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Press Unit
Unité de la Presse

Factsheet – Personal data protection

September 2018
This factsheet does not bind the Court and is not exhaustive

Personal data protection

¹The 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^{1]} ... 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.

¹. 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.”



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE



Court of Justice of the European Union

PRESS RELEASE No 81/18

Luxembourg, 5 June 2018

Judgment in Case C-210/16

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v
Wirtschaftsakademie Schleswig-Holstein GmbH

Press and Information

The administrator of a fan page on Facebook is jointly responsible with Facebook for the processing of data of visitors to the page

The data protection authority of the Member State in which the administrator has its seat may, under Directive 95/46,¹ act both against the administrator and against the Facebook subsidiary established in that Member State

The German company Wirtschaftsakademie Schleswig-Holstein operates in the field of education. It offers educational services inter alia by means of a fan page² hosted on Facebook at the address www.facebook.com/wirtschaftsakademie.

Administrators of fan pages, such as Wirtschaftsakademie, can obtain anonymous statistical data on visitors to the fan pages via a function called 'Facebook Insights' which Facebook makes available to them free of charge under non-negotiable conditions of use. The data is collected by means of evidence files ('cookies'), each containing a unique user code, which are active for two years and are stored by Facebook on the hard disk of the computer or on another device of visitors to the fan page. The user code, which can be matched with the connection data of users registered on Facebook, is collected and processed when the fan pages are opened.

By decision of 3 November 2011, the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent Data Protection Centre for the Land of Schleswig-Holstein, Germany), as supervisory authority within the meaning of Directive 95/46 on data protection, with the task of supervising the application in the Land of Schleswig-Holstein of the provisions adopted by Germany pursuant to that directive, ordered Wirtschaftsakademie to deactivate its fan page. According to the Unabhängiges Landeszentrum, neither Wirtschaftsakademie nor Facebook informed visitors to the fan page that Facebook, by means of cookies, collected personal data concerning them and then processed the data.

Wirtschaftsakademie brought an action against that decision before the German administrative courts, arguing that the processing of personal data by Facebook could not be attributed to it, and that it had not commissioned Facebook to process data that it controlled or was able to influence. Wirtschaftsakademie concluded that the Unabhängiges Landeszentrum should have acted directly against Facebook instead of against it.

It is in that context that the Bundesverwaltungsgericht (Federal Administrative Court, Germany) asks the Court of Justice to interpret Directive 95/46 on data protection.

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31). This directive was repealed with effect from 25 May 2018 by 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, OJ 2016 L 119, p. 1).

² Fan pages are user accounts that can be set up on Facebook by individuals or businesses. To do so, the author of the fan page, after registering with Facebook, can use the platform designed by Facebook to introduce himself to the users of that social network and to persons visiting the fan page, and to post any kind of communication in the media and opinion market.

www.curia.europa.eu

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 организует, координирует и поощряет проповедническую деятельность своих общин.

<http://curia.europa.eu/juris/celex.jsf?celex=62016CJ0210&lang1=en&type=TXT&ancre=>

<http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0025&lang1=en&type=TXT&ancre=>

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

ARRÊT 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^{mes} A. Prechal, C. Toader, MM. A. Rosas (rapporteur) et M. Ilešić, 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/ЕС, но ценна сама позиция суда и описание ситуации.



Press and Information

Court of Justice of the European Union
PRESS RELEASE No 125/19
Luxembourg, 1 October 2019

Judgment in Case C-673/17
Bundesverband der Verbraucherzentralen und Verbraucherverbände –
Verbraucherzentrale Bundesverband eV v Planet49 GmbH

Storing cookies requires internet users' active consent

A pre-ticked checkbox is therefore insufficient

The German Federation of Consumer Organisations has challenged before the German courts the use by the German company, Planet49, of a pre-ticked checkbox in connection with online promotional games, by which internet users wishing to participate consent to the storage of cookies.¹ The cookies in question aim to collect information for the purposes of advertising Planet49's partners' products.

The Bundesgerichtshof (Federal Court of Justice, Germany) asked the Court of Justice to interpret the EU law on the protection of electronic communications privacy.²

In today's judgment, the Court decides that the consent which a website user must give to the storage of and access to cookies on his or her equipment is not validly constituted by way of a pre-checked checkbox which that user must deselect to refuse his or her consent.

That decision is unaffected by whether or not the information stored or accessed on the user's equipment is personal data. EU law aims to protect the user from any interference with his or her private life, in particular, from the risk that hidden identifiers and other similar devices enter those users' terminal equipment without their knowledge.

The Court notes that consent must be specific so that the fact that a user selects the button to participate in a promotional lottery is not sufficient for it to be concluded that the user validly gave his or her consent to the storage of cookies.

Furthermore, according to the Court, the information that the service provider must give to a user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

¹ Cookies are files which the provider of a website stores on the website user's computer which that website provider can access again when the user visits the website on a further occasion, in order to facilitate navigation on the internet or transactions, or to access information about user behaviour.

² Directive 2002/58/EC of the European Parliament and of the Council 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) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11), read in conjunction with Article 2(h) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), and of Article 6(1)(a) 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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

www.curia.europa.eu

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.

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf>

<https://edri.org/cjeu-cookies-consent-or-be-tracked-not-an-option/>



Reports of Cases

JUDGMENT OF THE COURT (Third Chamber)

11 December 2019*

[Text rectified by order of 13 February 2020]

(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Charter of Fundamental Rights of the European Union — Articles 7 and 8 — Directive 95/46/EC — Article 6(1)(c) and Article 7(f) — Making the processing of personal data legitimate — National legislation allowing video surveillance for the purposes of ensuring the safety and protection of individuals, property and valuables and for the pursuit of legitimate interests, without the data subject's consent — Installation of a video surveillance system in the common parts of a residential building)

In Case C-708/18,

REQUEST for a preliminary ruling under Article 267 TFEU from Tribunalul București (Regional Court, Bucharest, Romania), made by decision of 2 October 2018, received at the Court on 6 November 2018, in the proceedings

TK

v

Asociația de Proprietari bloc M5A-ScaraA,

THE COURT (Third Chamber),

composed of A. Prechal (Rapporteur), President of the Chamber, L.S. Rossi, J. Malenovský, F. Biltgen and N. Wahl, Judges,

Advocate General: G. Pitruzzella,

Registrar: A. Calot Escobar,

having regard to the written procedure,

after considering the observations submitted on behalf of:

- the Romanian Government, by C.-R. Canțâr, O.-C. Ichim and A. Wellman, acting as Agents,
- the Czech Government, by M. Smolek, J. Vláčil and O. Serdula, acting as Agents,
- the Danish Government, by J. Nymann-Lindegren, M. Wolff and P.Z.L. Ngo, acting as Agents,

* Language of the case: Romanian.

ECLI:EU:C:2019:1064

Court of Justice of the European Union

*Judgment in Case Case C-708/18
TK v Asociația de Proprietari bloc M5A-ScaraA*

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
PRESS RELEASE No 88/20
Luxembourg, 9 July 2020

Judgment in Case C-264/19

Press and Information

Constantin Film Verleih GmbH v YouTube LLC and Google Inc.

When a film is unlawfully uploaded onto an online platform, such as YouTube, the rightholder may, under the directive on the enforcement of intellectual property rights, require the operator to provide only the postal address of the user concerned, but not his or her email, IP address or telephone number

In the judgment in *Constantin Film Verleih* (C-264/19), delivered on 9 July 2020, the Court ruled that, where a film is uploaded onto an online video platform without the copyright holder's consent, Directive 2004/48¹ does not oblige the judicial authorities to order the operator of the video platform to provide the email address, IP address or telephone number of the user who uploaded the film concerned. The directive, which provides for disclosure of the 'addresses' of persons who have infringed an intellectual property right, covers only the postal address.

In 2013 and 2014, the films *Parker* and *Scary Movie 5* were uploaded onto the video platform YouTube without the consent of Constantin Film Verleih, the holder of the exclusive exploitation rights in respect of those works in Germany. Those films have been viewed tens of thousands of times. Constantin Film Verleih then demanded that YouTube and Google, the latter being the parent company of the former, with which users must first register by means of a user account, provide it with a set of information relating to each of the users who had uploaded those films. The two companies refused to provide Constantin Film Verleih with information about those users, in particular their email addresses and telephone numbers, as well as the IP addresses used by them, both at the time when the files concerned were uploaded and when they last accessed their Google/YouTube account.

The dispute in the main proceedings hinged on whether such information is covered by the term 'addresses' within the meaning of Directive 2004/48. That directive provides that judicial authorities may order disclosure of information on the origin and distribution networks of the goods or services which infringe an intellectual property right. That information includes, *inter alia*, the 'addresses' of producers, distributors and suppliers of the infringing goods or services.

The Court found, in the first place, that, as regards the usual meaning of the term 'address', it refers only to the postal address, that is to say, the place of a given person's permanent address or habitual residence. It follows that that term, when it is used without any further clarification, as in Directive 2004/48, does not refer to the email address, telephone number or IP address. In the second place, the *travaux préparatoires*² that led to the adoption of Directive 2004/48 contain nothing to suggest that the term 'address' should be understood as referring not only to the postal address but also to the email address, telephone number or IP address of the persons concerned. In the third place, an examination of other EU legal acts referring to email addresses or IP addresses reveals that none of them uses the term 'address', without further details, to designate the telephone number, IP address or email address.

¹ Article 8(2)(a) of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum OJ 2004 L 195, p. 18).

² Proposal for a Directive of the European Parliament and of the Council on measures and procedures to ensure the enforcement of intellectual property rights of 30 January 2003 (COM(2003) 46 final), Opinion of the European Economic and Social Committee of 29 October 2003 (OJ 2004 C 32, p. 15) and Report of 5 December 2003 by the European Parliament (A5 0468/2003) on that proposal.

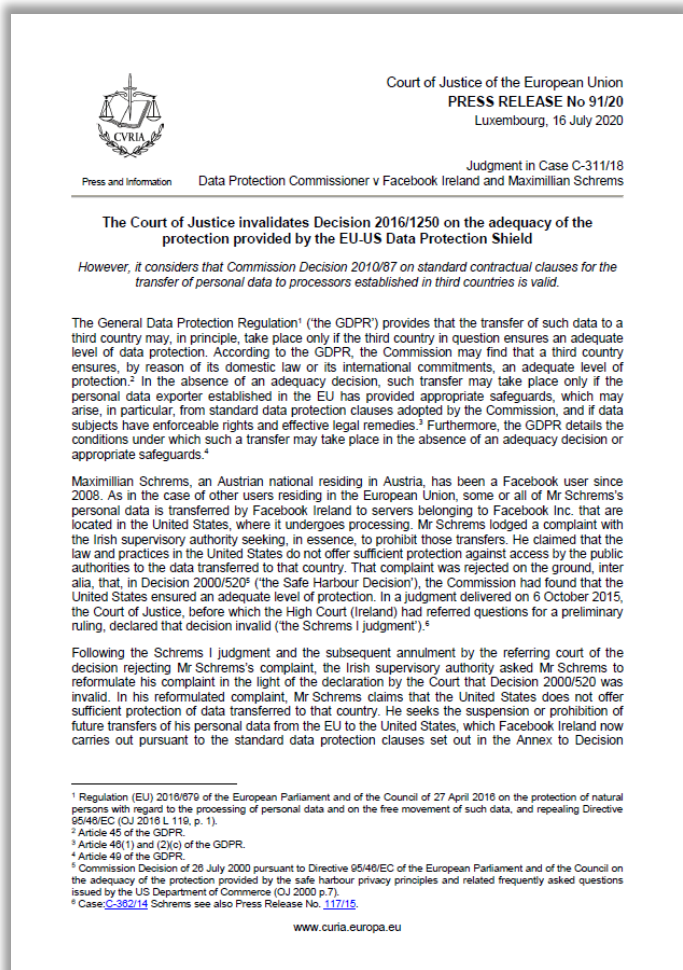
www.curia.europa.eu

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.



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.



Press and Information

Court of Justice of the European Union
PRESS RELEASE No 123/20
Luxembourg, 6 October 2020

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*

The Court of Justice confirms that EU law precludes national legislation requiring a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security

However, in situations where a Member State is facing a serious threat to national security that proves to be genuine and present or foreseeable, that Member State may derogate from the obligation to ensure the confidentiality of data relating to electronic communications by requiring, by way of legislative measures, the general and indiscriminate retention of that data for a period that is limited in time to what is strictly necessary, but which may be extended if the threat persists. As regards combating serious crime and preventing serious threats to public security, a Member State may also provide for the targeted retention of that data as well as its expedited retention. Such an interference with fundamental rights must be accompanied by effective safeguards and be reviewed by a court or by an independent administrative authority. Likewise, it is open to a Member State to carry out a general and indiscriminate retention of IP addresses assigned to the source of a communication where the retention period is limited to what is strictly necessary, or even to carry out a general and indiscriminate retention of data relating to the civil identity of users of means of electronic communication, and in the latter case the retention is not subject to a specific time limit

In recent years, the Court of Justice has ruled, in several judgments, on the retention of and access to personal data in the field of electronic communications.¹ The resulting case-law, in particular the judgment in *Tele2 Sverige and Watson and Others*, in which the Court held, inter alia, that Member States could not require providers of electronic communications services to retain traffic data and location data in a general and indiscriminate way, has caused concerns on the part of certain States that they may have been deprived of an instrument which they consider necessary to safeguard national security and to combat crime.

¹ Thus, in the judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-203/12 and C-584/12) (see [Press Release No 54/14](#)), the Court declared Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), invalid on the ground that the interference with the rights to respect for private life and to the protection of personal data, recognised by the Charter of Fundamental Rights of the European Union ('the Charter'), which resulted from the general obligation to retain traffic data and location data laid down by that directive was not limited to what was strictly necessary. In the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15) (see [Press Release No 145/16](#)), the Court then interpreted Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council 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) (OJ 2002 L 201, p. 37), as amended by Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('the directive on privacy and electronic communications'). That article empowers the Member States – on grounds of the protection, inter alia, of national security – to adopt 'legislative measures' intended to restrict the scope of certain rights and obligations provided for in the directive. Lastly, in the judgment of 2 October 2018, *Ministerio Fiscal* (C-207/18) (see [Press Release No 141/18](#)), the Court interpreted Article 15(1) of that directive in a case which concerned public authorities' access to data relating to the civil identity of users of means of electronic communication.

www.curia.europa.eu

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.



Court of Justice of the European Union
PRESS RELEASE No 137/20
Luxembourg, 11 November 2020

Judgment in Case C-61/19
Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării
Datelor cu Caracter Personal (ANSPDCP)

Press and Information

A contract for the provision of telecommunications services containing a clause stating that the customer has consented to the collection and storage of his or her identity document cannot demonstrate that that customer has validly given his or her consent where the box referring to that clause has been ticked by the data controller before the contract was signed

That is also the case where the customer is misled as to the possibility of concluding the contract if he or she refuses to consent to the processing of his or her data, or where the freedom to choose to object to that collection and storage is affected by the requirement to complete an additional form setting out that refusal

Orange România SA is a provider of mobile telecommunications services on the Romanian market. On 28 March 2018, the Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (the National Authority for the Supervision of Personal Data Processing), imposed a fine on it for collecting and storing copies of its customers' identity documents without their express consent.

According to that ANSPDCP, between 1 and 26 March 2018, Orange România had concluded contracts for the provision of mobile telecommunications services which contain a clause stating that customers have been informed of, and have consented to, the collection and storage of a copy of their identity documents for identification purposes. The box relating to that clause had been ticked by the data controller before the contract was signed.

It is in that context that the Tribunalul București (Regional Court, Bucharest, Romania) requested the Court of Justice to specify the conditions in which the customers' consent to the processing of personal data may be considered valid.

By its judgment today, the Court notes, first of all, that EU law¹ provides for a list of the cases in which the processing of personal data can be regarded as being lawful. In particular, the data subject's consent must be freely given, specific, informed and unambiguous. In that regard, consent is not validly given in the case of silence, pre-ticked boxes or inactivity.

In addition, if the data subject's consent is given in the context of a written declaration which also concerns other matters, that declaration must be presented in an intelligible and easily accessible form, using clear and plain language. In order to ensure that the data subject enjoys genuine freedom of choice, the contractual terms must not mislead him or her as to the possibility of concluding the contract even if he or she refuses to consent to the processing of his or her data.

The Court points out that since Orange România is the controller of personal data, it must be able to demonstrate the lawfulness of the processing of those data and therefore, in the present case, the existence of the valid consent of its customers. In that regard, given that the customers concerned do not appear to have themselves ticked the box relating to the collection and storage

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) and 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 (OJ 2016 L 119, p. 1)

www.curia.europa.eu

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).

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.

TRIBUNAL ADMINISTRATIF DE MARSEILLE

N° 1901249

RÉPUBLIQUE FRANÇAISE

LA QUADRATURE DU NET
et autres

AU NOM DU PEUPLE FRANÇAIS

M. Youssef Khiat
Rapporteur

Le tribunal administratif de Marseille

(9^{ème} chambre)M. Pierre-Yves Gonneau
Rapporteur publicAudience du 3 février 2020
Lecture du 27 février 202026-07-01-02
135-04-02-01-01
C+

Vu la procédure suivante :

Par une requête, enregistrée le 14 février 2019, l'association « La Quadrature du Net » et la Ligue des droits de l'Homme, la fédération des conseils des parents d'élèves des écoles publiques des Alpes-Maritimes et le syndicat CGT Educ'Action des Alpes-Maritimes, représentés par Me Alexis Fitzjean O Cobhthaigh, demandant au Tribunal :

1°) d'annuler pour excès de pouvoir la délibération n° 18-893 du 14 décembre 2018 par laquelle le conseil régional de Provence-Alpes-Côte d'Azur a approuvé la convention tripartite d'expérimentation région-lycée-société Cisco International Limited relative à la mise en place d'un dispositif de contrôle d'accès par comparaison faciale et de suivi de trajectoire, a autorisé son président à signer cette convention et a lancé cette expérimentation au sein des lycées Ampère (Marseille) et Les Eucalyptus (Nice) ;

2°) de mettre à la charge de la région Provence-Alpes-Côte d'Azur la somme de 1 024 euros au titre de l'article L. 761-1 du code de justice administrative.

Elles soutiennent que :

- la délibération attaquée est entachée d'incompétence : concernant la sécurité à l'entrée des lycées, elle relève de la compétence des seuls chefs d'établissement ;
- elle est entachée d'un vice de procédure en ce qu'elle autorise la mise en œuvre d'un traitement de données biométriques alors qu'aucune étude d'impact n'a été réalisée au moment de son adoption, nuisant à la bonne information de la population et du conseil régional ;



de Rechtspraak

Home Onderwerpen Uitspraken en nieuws Registers **de Rechtspraak** Professionals

[Rechtbank Midden-Nederland](#) > [Nieuws](#) > VoetbalTV hoeft boete Autoriteit Persoonsgegevens niet te betalen

VoetbalTV hoeft boete Autoriteit Persoonsgegevens niet te betalen

Utrecht, 23 november 2020

VoetbalTV heeft een boete van €575.000 van de Autoriteit Persoonsgegevens gekregen, maar hoeft die van de rechtbank niet te betalen. De Autoriteit Persoonsgegevens heeft volgens de rechtbank onvoldoende uitgelegd waarom VoetbalTV geen gerechtvaardigd belang heeft bij het opnemen en uitzenden van amateurwedstrijden. De Autoriteit Persoonsgegevens moet van de rechtbank nog onderzoeken of het belang van VoetbalTV bij het opnemen en uitzenden van wedstrijden in overeenstemming is met de privacyregels.

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.

JD SUPRA®

August 31, 2018

German Art Copyright Act Applies Even With GDPR In Effect



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.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

d'AMICO DRY d.a.c., f/k/a d'Amico Dry :
Limited, :
Plaintiff, :
vs. : CA 18-0284-KD-MU
NIKKA FINANCE, INC., as owner of the : IN ADMIRALTY
M/V SEA GLASS II, :
Defendant.

ORDER

This cause is before the undersigned on Defendant's motion for protective order (Doc. 123) and Plaintiff's response (Doc. 134).¹ This order **DENYING** Defendant's motion for protective order is entered pursuant to 28 U.S.C. § 636(b)(1)(A) and General Local Rule 72(a)(2)(S).²

FACTUAL BACKGROUND

This admiralty action has been pending in this Court since June 22, 2018, based upon d'Amico's verified complaint against Defendant Nikka and the within Rule B

¹ Nikka was extended the opportunity to file a reply by October 16, 2018 (Doc. 130) but did not do so (*compare id. with* Docket Sheet).

² Although the undersigned is denying the motion for protective order and allowing Paul Coronis' deposition to be videotaped in London, England on October 24, 2018, in recognition of the privacy interests Mr. Coronis has identified the undersigned is specifically **ORDERING** that the video recording component of Mr. Coronis' deposition can only be used in these civil proceedings in this Court and is **NOT** to be publically disclosed or used in any other investigation or litigation.



The screenshot shows the BBC News website interface. At the top, there is a navigation bar with the BBC logo, a 'Sign in' button, and menu items for News, Sport, Reel, Worklife, Travel, and Future. Below this is a red banner with the word 'NEWS' in white. Underneath the banner is another navigation bar with links for Home, Video, World, UK, Business, Tech, Science, Stories, and Entertainment & Arts. The main content area features the article title 'Google wins landmark right to be forgotten case' in large, bold black text. Below the title, 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. A subsequent paragraph mentions that in 2015, CNIL ordered Google to globally remove search result listings to pages containing damaging or false information about a person. Another paragraph notes that the following year, Google introduced a geoblocking feature to prevent European users from seeing delisted links. The final paragraph states that Google resisted censoring search results for people in other parts of the world and challenged a 100,000 euro fine imposed by CNIL.

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.

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 Conroy | May 10, 2019, 3:37 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 *Closest* 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

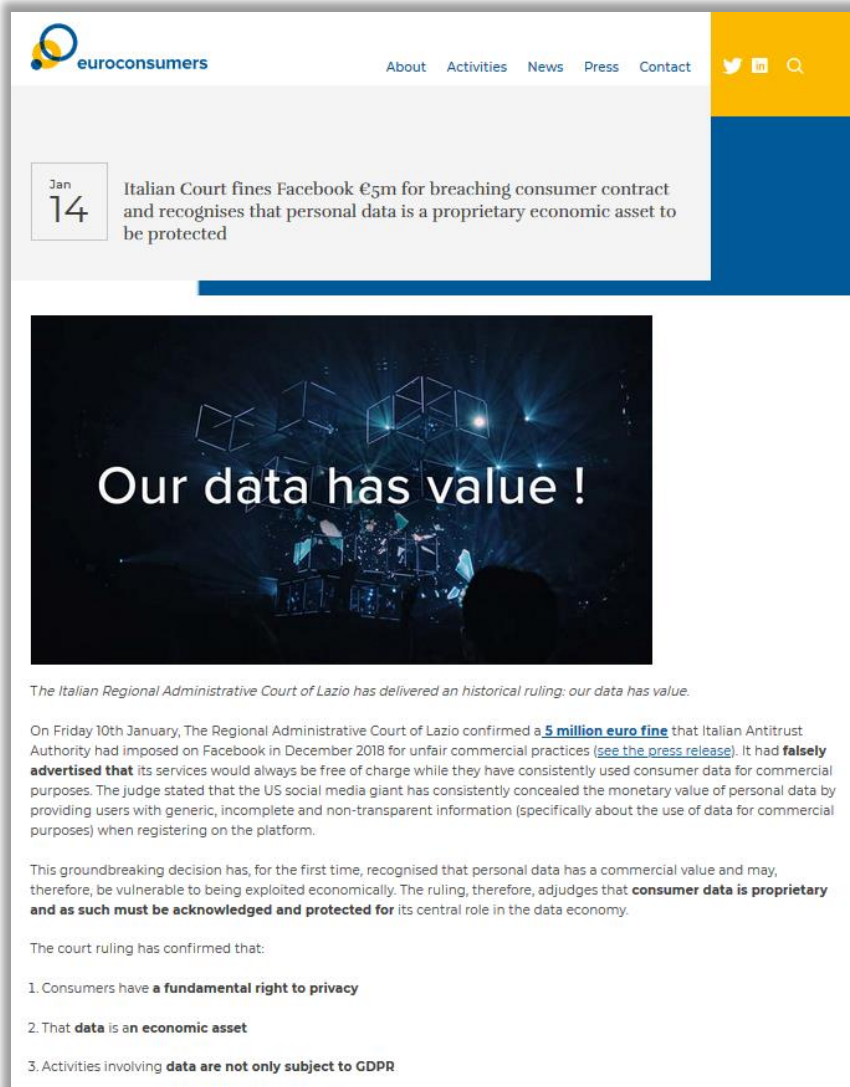
German court decides that GDPR consent can be tied to receiving advertising

*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».



The screenshot shows the website of euroconsumers. At the top left is the logo and name 'euroconsumers'. To the right are navigation links: 'About', 'Activities', 'News', 'Press', 'Contact'. Further right are social media icons for Twitter, Facebook, and a search icon. Below the navigation is a date box for 'Jan 14' and a headline: 'Italian Court fines Facebook €5m for breaching consumer contract and recognises that personal data is a proprietary economic asset to be protected'. The main content area features a large image with the text 'Our data has value!' and a list of three points confirming the court's ruling.

Our data has value !

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.



U bent hier: Home > Uitspraken > Uitspraak 201902699/1/A2

Uitspraak 201902699/1/A2

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.

eerste aanleg - meervoudig 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.

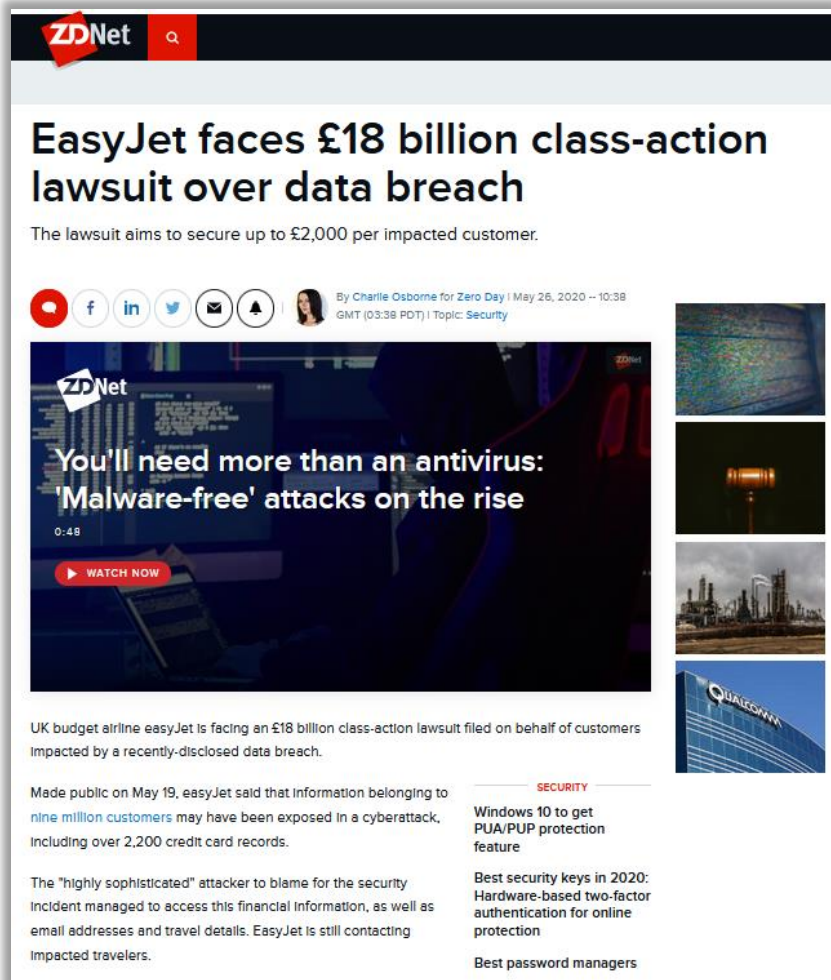


The image shows a screenshot of a BBC News article. At the top, the BBC logo is visible on the left, and navigation links for 'Sign in', 'News', 'Sport', 'Reel', 'Worklife', 'Travel', and 'Future' are on the right. Below this is a red header with the word 'NEWS' in white. Underneath, there are more navigation 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, a short summary states: '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 Общего регламента Евросоюза по защите данных (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.



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.

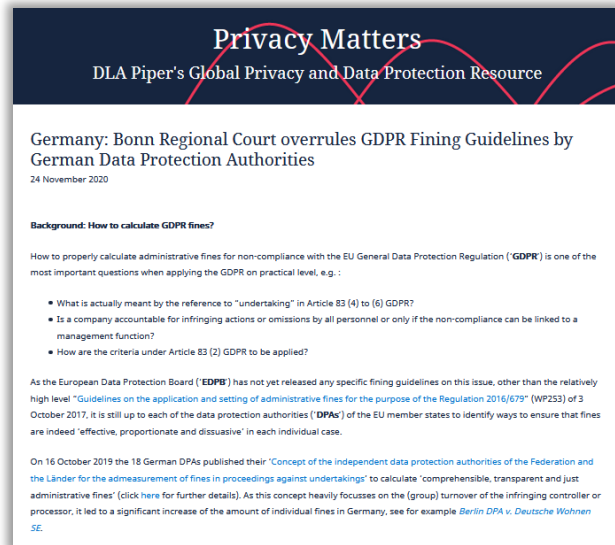
The "highly sophisticated" attacker to blame for the security incident managed to access this financial information, as well as email addresses and travel details. EasyJet is still contacting impacted travelers.

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.



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.

Влияние GDPR на бизнес



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>

- ❖ [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

TechGenYZ TG NOW ▾ TECH ▾ FUTURE ▾ GAMING ▾ HOW TO ▾ PHONE FINDER DEALS REVIEWS

Seven European Union countries accuse Google of GDPR violations

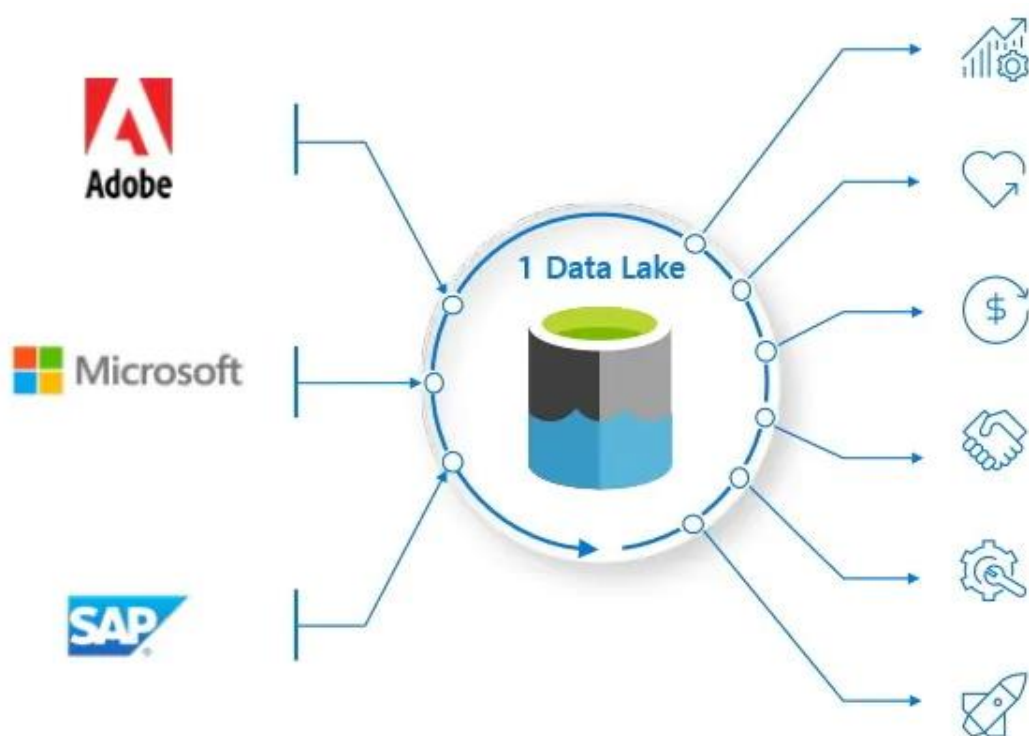
By Oindrila Banerjee
Nov 27, 2018, 4:30 Pm



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.

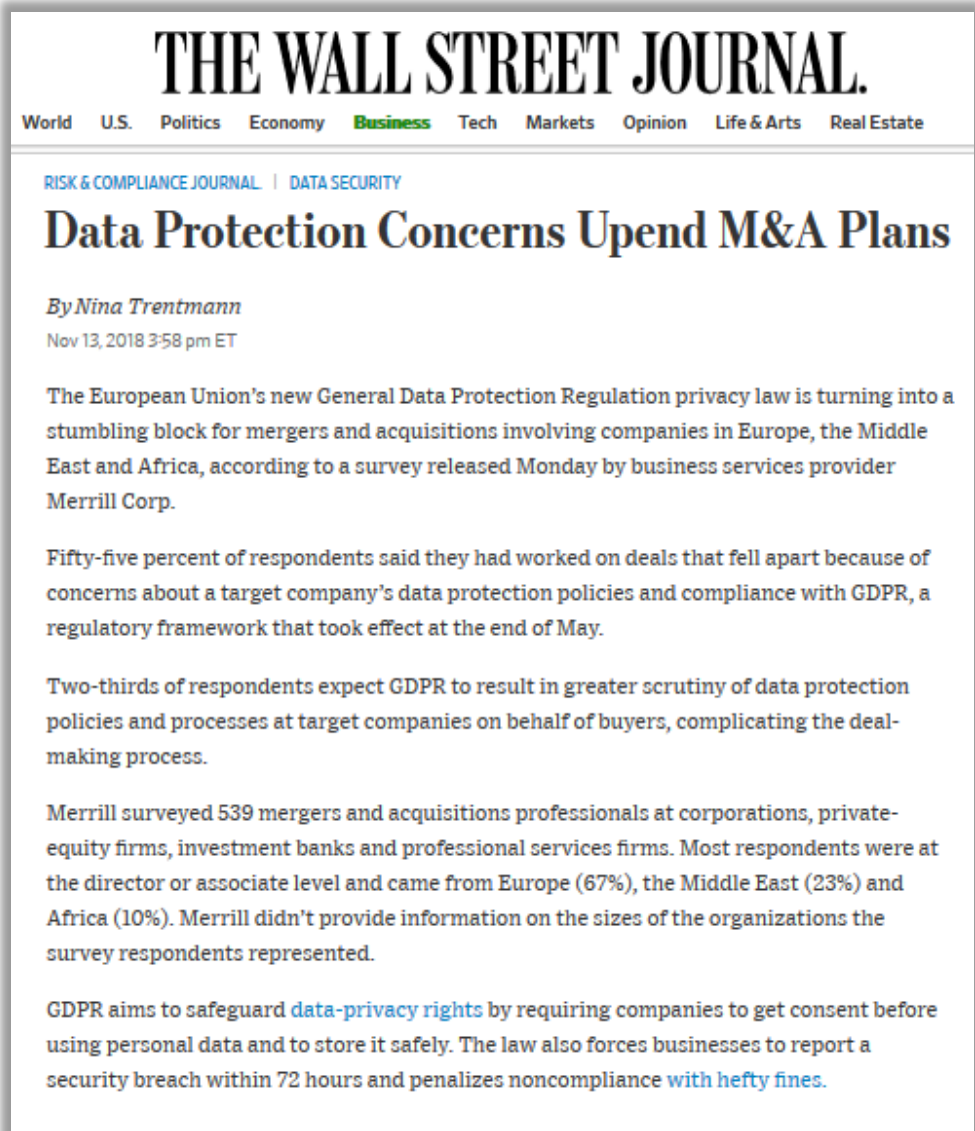


Производители программного обеспечения SAP и Adobe Systems, а также американская корпорация Microsoft заявили о создании альянса Open Data Initiative, призванного обеспечить эффективное использование всех данных о клиентах, собираемых разными приложениями через разные каналы (онлайновые и офлайновые), 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>



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.

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



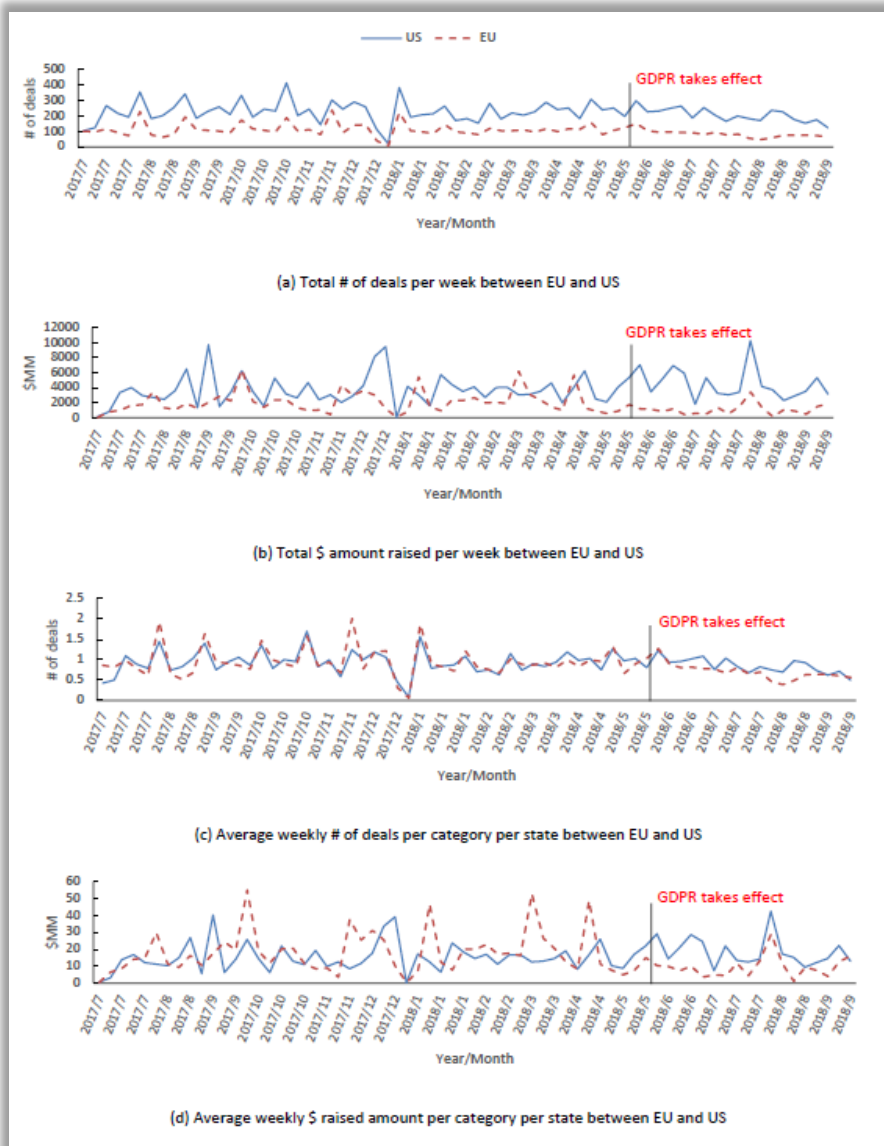
Björn Greif
Editor

[Blog](#)

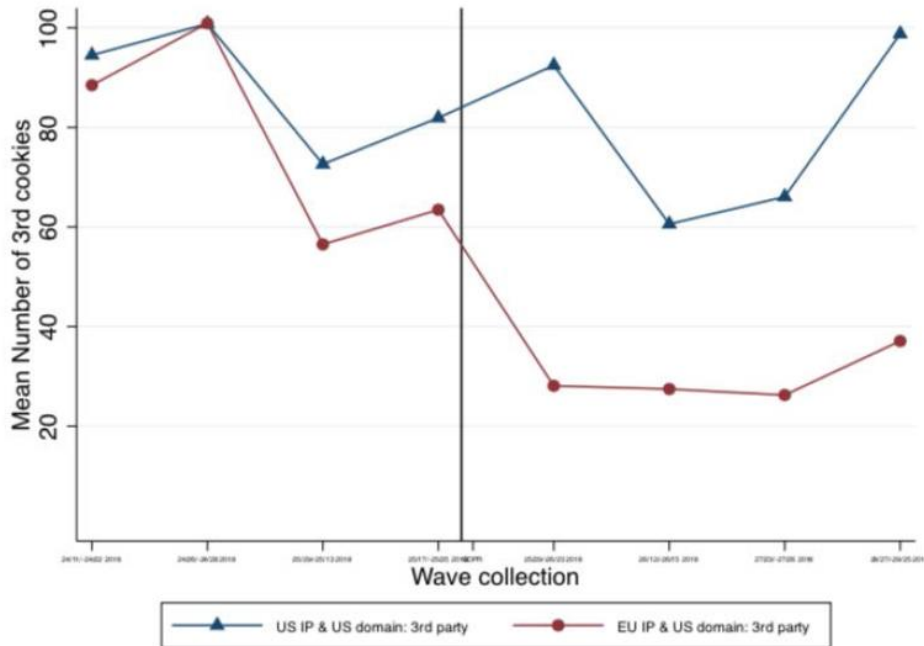
The [General Data Protection Regulation](#) (GDPR), which primarily aims to protect personal data within the EU, has been in effect for a little over four months now. But what has changed since 25th of May? What impact did the GDPR have on the tracker landscape and the online advertising market in Europe? 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.



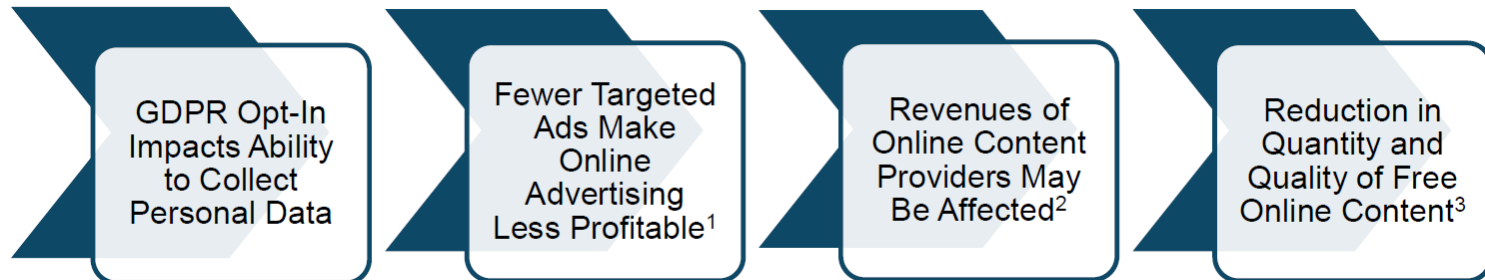
Согласно выводам исследования National Bureau of Economic Research, GDPR оказал негативное влияние на европейские стартапы по сравнению их американскими коллегами. Например, общий объем венчурного капитала, инвестированного в стартапы ЕС, упал на 50% из-за внедрения GDPR. Кроме того, на 17,6% сократилось количество еженедельных венчурных сделок и на 39,6% уменьшилось количество привлеченных средств в среднем на каждую сделку.



Number 3rd 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.





Hacking News ▾ Tech ▾ Cyber Crime ▾ How To ▾ Cyber Events ▾ Security ▾ Surveillance ▾ Explore ▾

You are here: Home » Cyber Crime » Ransomhack; a new attack blackmailing business owners using GDPR

Ransomhack; a new attack blackmailing business owners using GDPR

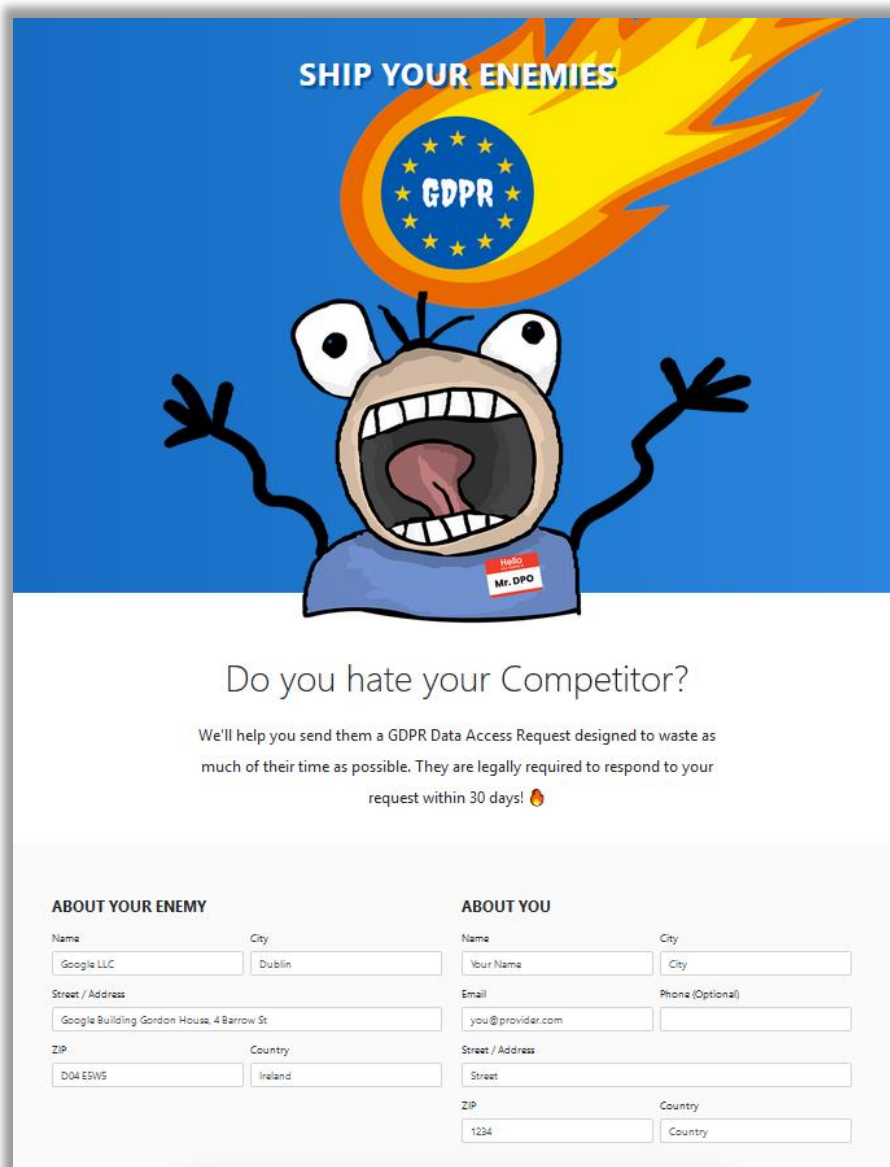
By Waqas on June 23, 2018 [Email](#) [@hackread](#) [CYBER CRIME](#) [HACKING-NEWS](#)



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.



The image shows a screenshot of the 'Ship Your Enemies' website. At the top, there's a blue banner with the text 'SHIP YOUR ENEMIES' and a graphic of a fireball with the GDPR logo (a blue circle with yellow stars and the text 'GDPR') inside it. Below the banner is a cartoon character with a wide, toothy grin and a name tag that says 'Hello Mr. DPO'. The main text asks 'Do you hate your Competitor?' and explains that the service helps send GDPR Data Access Requests designed to waste as much of the competitor's time as possible. Below this is a form with two columns: 'ABOUT YOUR ENEMY' and 'ABOUT YOU'. The 'ABOUT YOUR ENEMY' column has fields for Name (Google LLC), City (Dublin), Street / Address (Google Building Gordon House, 4 Barrow St), ZIP (D04 E5W5), and Country (Ireland). The 'ABOUT YOU' column has fields for Name (Your Name), City, Email (you@provider.com), Phone (Optional), Street / Address, Street, ZIP (1234), and Country.

SHIP YOUR ENEMIES

GDPR

Hello
Mr. DPO

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: Google LLC City: Dublin

Street / Address: Google Building Gordon House, 4 Barrow St

ZIP: D04 E5W5 Country: Ireland

ABOUT YOU

Name: Your Name City: City

Email: you@provider.com Phone (Optional):

Street / Address: Street

ZIP: 1234 Country: 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.

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.

Weaponizing the GDPR

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».

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).



REUTERS Business Markets World Politics TV More

TECHNOLOGY NEWS FEBRUARY 19, 2020 / 10:55 PM / UPDATED 14 HOURS AGO

Exclusive: Google users in UK to lose EU data protection - sources

Joseph Menn

The shift, prompted by Britain's exit from the EU, will leave the sensitive personal information of tens of millions with less protection and within easier reach of British law enforcement.

The change was described to Reuters by three people familiar with its plans. Google intends to require its British users to acknowledge new terms of service including the new jurisdiction.

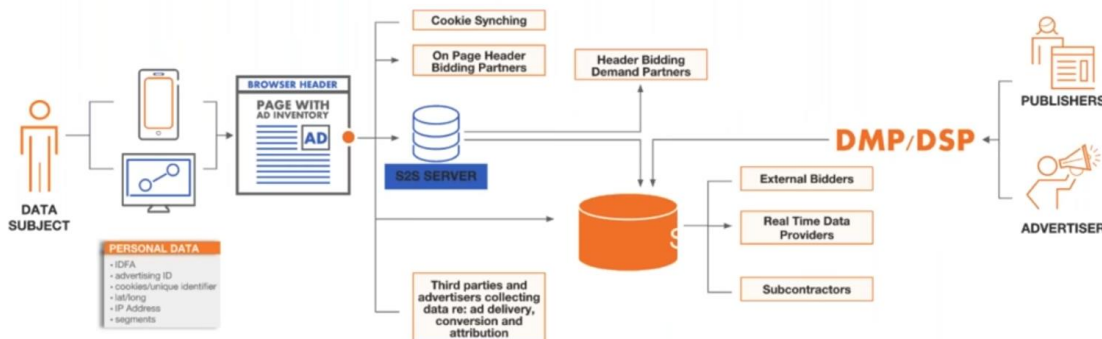
Ireland, where Google and other U.S. tech companies have their European headquarters, is staying in the EU, which has one of the world's most aggressive data protection rules, the General Data Protection Regulation.

Google has decided to move its British users out of Irish jurisdiction because it is unclear whether Britain will follow GDPR or adopt other rules that could affect the handling of user data, the people said.

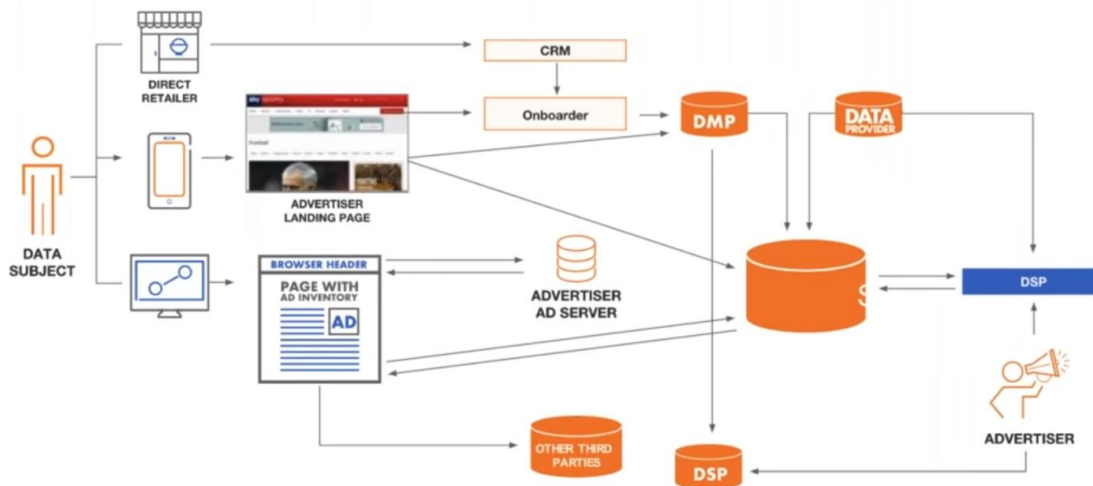
If British Google users have their data kept in Ireland, it would be more difficult for British authorities to recover it in criminal investigations.

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.

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.

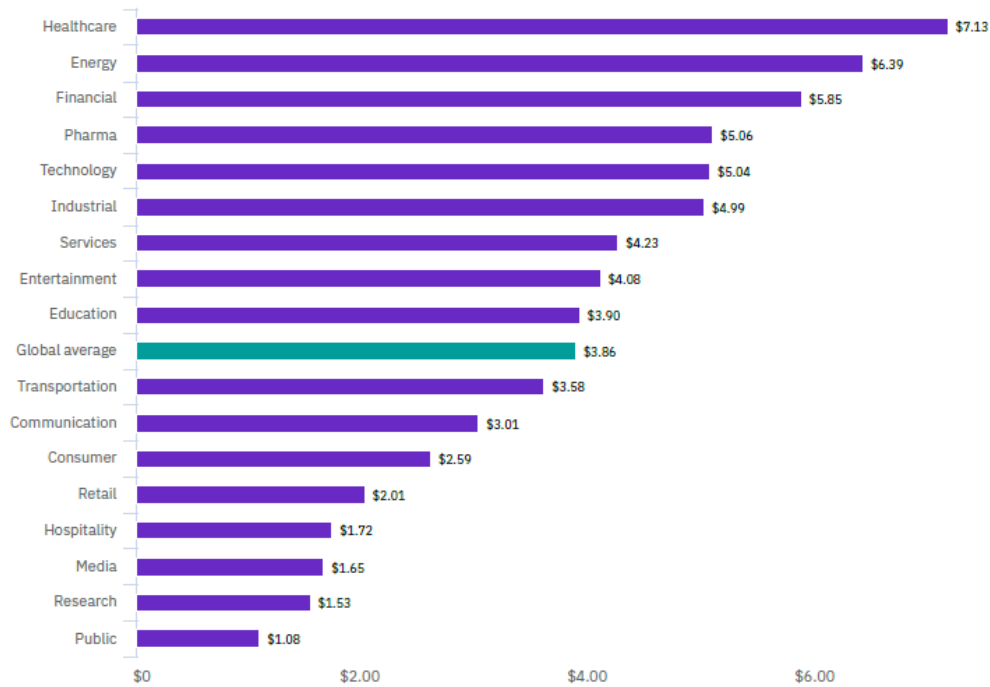
Некоторые сайты и медиаплатформы хотят убрать вторую опцию. Но тогда Google не сможет анализировать поведение пользователей, чтобы показывать им таргетированную рекламу. Поэтому Google требует, чтобы сайты, зарабатывающие на Google Ads, вынуждали пользователей давать оба согласия.

412 Отчет IBM от 2020 года о стоимости утечек данных



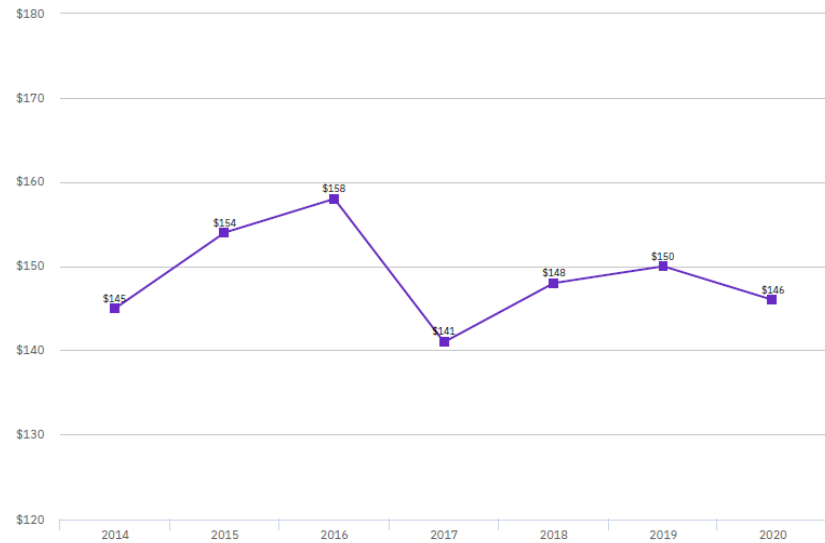
Average total cost of a data breach by industry

Measured in US\$ millions



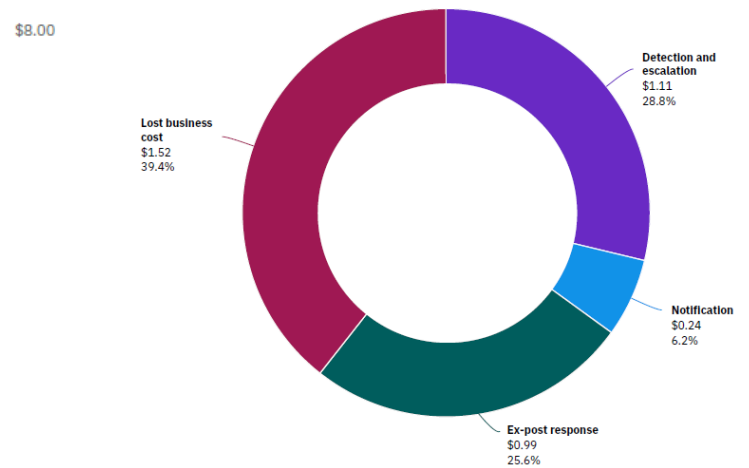
Average per record cost of a data breach

Measured in US\$



Data breach average total cost divided into four categories

Measured in US\$ millions



<https://www.ibm.com/security/data-breach>

<https://www.ibm.com/security/digital-assets/cost-data-breach-report>

От конфиденциальности к прибыли: достижение положительного дохода от инвестиций в приватность

Figure 1 Annual privacy spending overall and by company size
N=2549

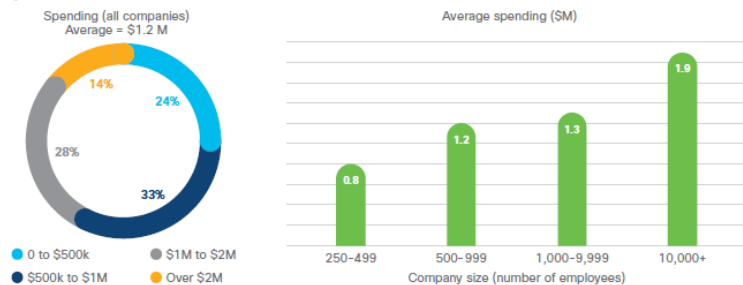


Figure 3 Estimated privacy benefits overall and by company size
N=2549

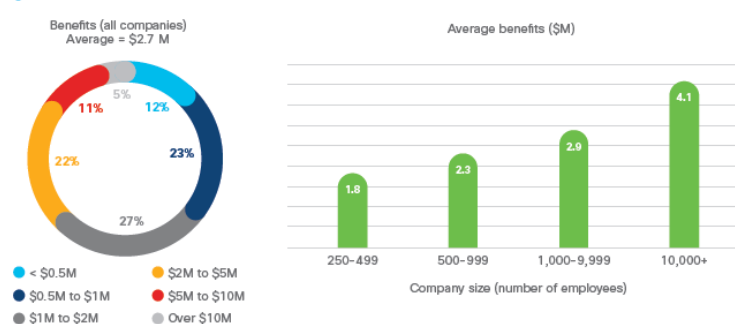


Figure 5 Average privacy returns by country
Global average: Benefits = 2.7 times investment
N=2543



Figure 2 Business impact of privacy
Percentage of companies getting significant benefits in each area, N=2549

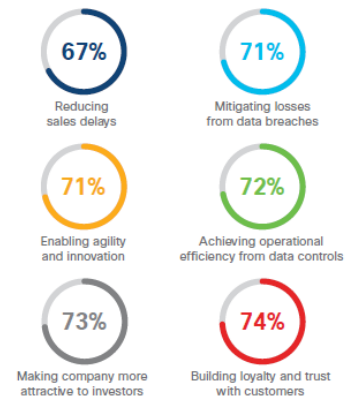
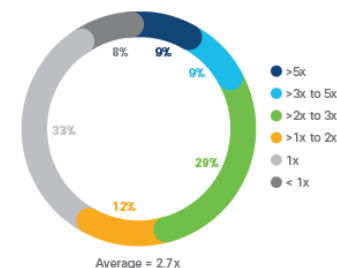


Figure 4 Distributions of privacy returns, percent of respondents
N=2543



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.

Итоги применения GDPR в 2018-2020 и дальнейшие перспективы





В феврале 2019 года отчёт о результатах правоприменительной практики GDPR выпустил Европейский совет по защите данных (EDPB). За время действия регламента европейские регуляторные органы открыли около 206 тысяч дел о нарушении безопасности персональных данных, а также наложили €55,955,871 штрафов. Почти половина из них (94 622) — по жалобам частных лиц. Ещё 64 864 дела открыли по уведомлению об утечке данных от компаний-виновников происшествия.

Большая часть из €56 млн. штрафов приходится на Google, которого в январе 2019 года французский регуляторный орган CNIL оштрафовал на €50 млн.

2019 ANNUAL REPORT

WORKING TOGETHER FOR STRONGER RIGHTS



edpb
European Data Protection Board

5	EUROPEAN DATA PROTECTION BOARD ACTIVITIES IN 2019	12
5.1.	General guidance	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.	Consistency Opinions	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.	Legislative consultation	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
6	SUPERVISORY AUTHORITY ACTIVITIES IN 2019	28
6.1.	Cross-border cooperation	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.	National cases	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.	SA survey on budget and staff	37
8	MAIN OBJECTIVES FOR 2020	40
8.1.	Legal work plan	40
8.1.1.	Guidance	40
8.1.2.	Advisory role to the European Commission	40
8.1.3.	Consistency findings	41
8.2.	Communications	41



Brussels, 24.6.2020
COM(2020) 264 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL

Data protection as a pillar of citizens' empowerment and the EU's approach to the
digital transition - two years of application of the General Data Protection Regulation

{SWD(2020) 115 final}

EN

EN

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.

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](#))

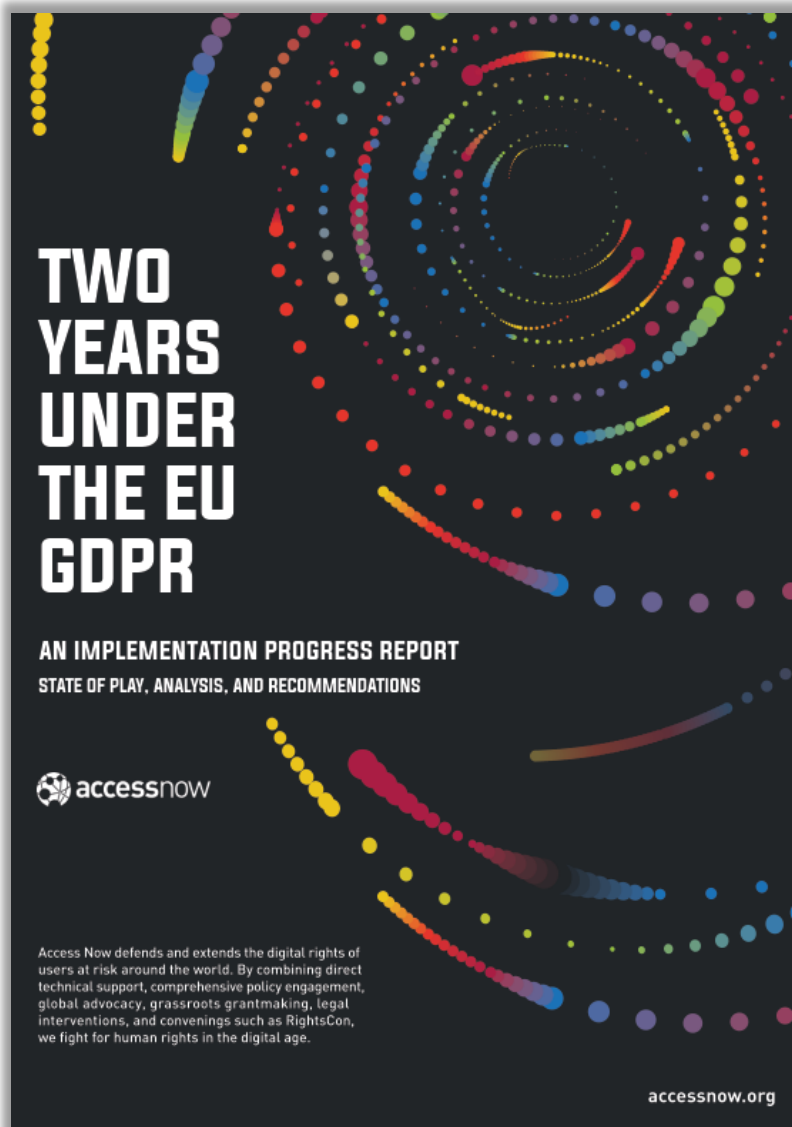
Ст.21 GDPR: Право отказаться (opt out) от обработки данных

- 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](#))

- 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, позволяют 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)

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:

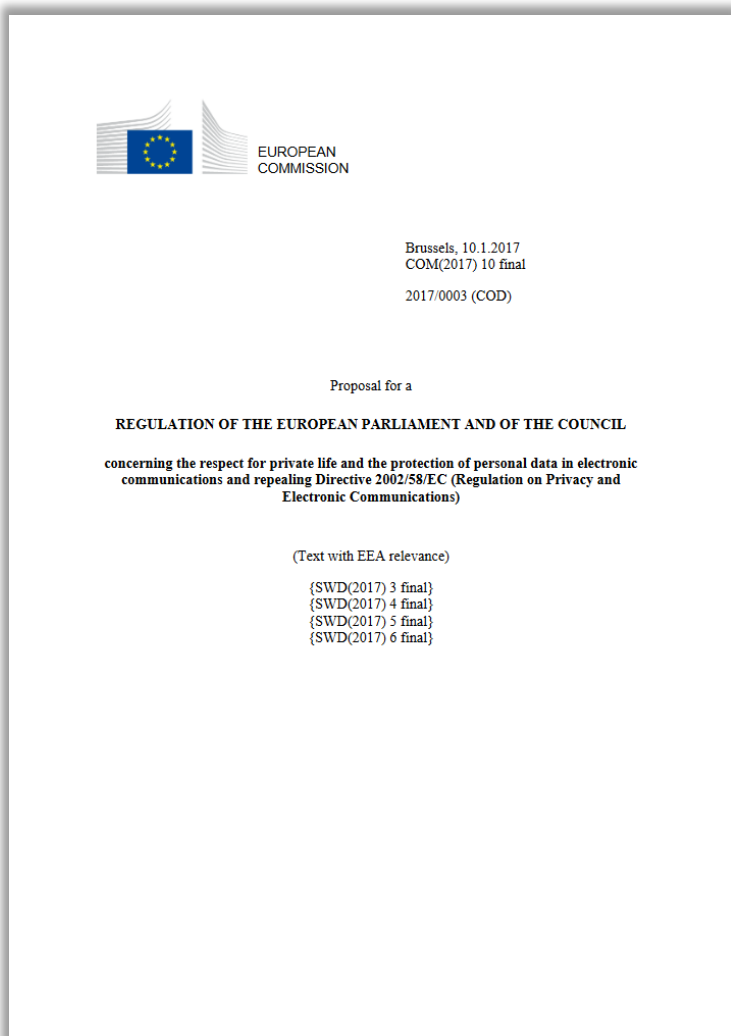
- за два года регуляторы наложили 231 штрафа, а получено было 144 376 жалоб субъектов;
- из 30 регуляторов из 27 стран ЕС только 9 довольны уровнем своего ресурсного обеспечения;
- в Польше, Румынии, Венгрии и Словакии суды и власть злоупотребляют GDPR, чтобы ограничить журналистские расследования;
- 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 UK 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.

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





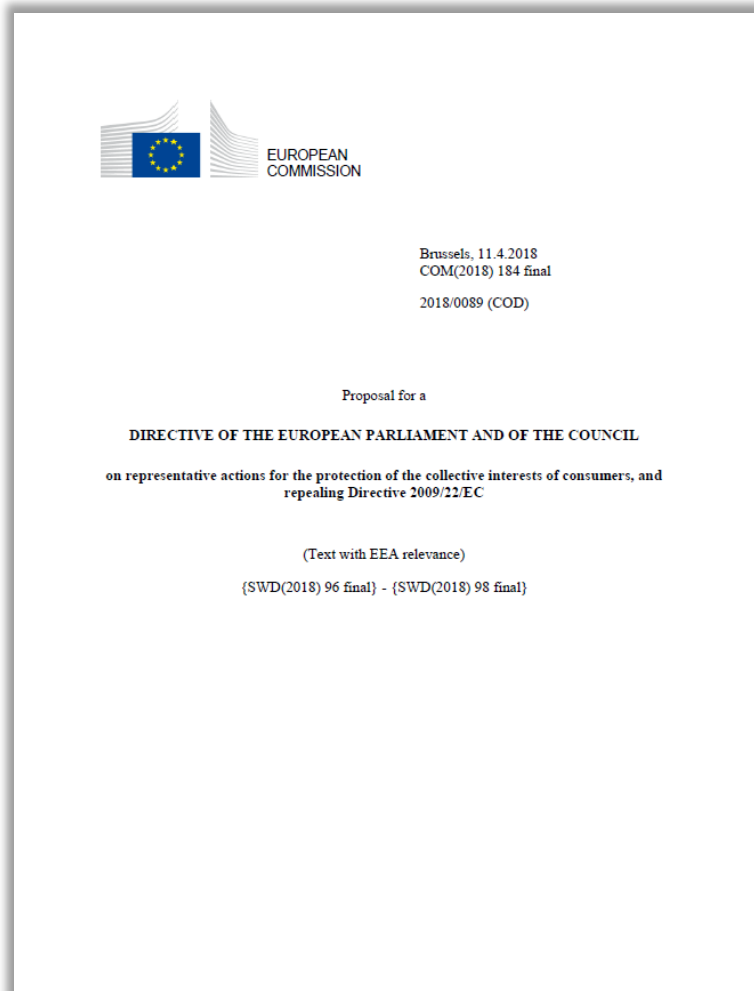
[Proposal 2017/0003 \(COD\) for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC \(Regulation on Privacy and Electronic Communications\)](#)

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:

- [Текущий статус рассмотрения проекта](#)
- [Общее описание целей, задач, структуры и содержания проекта](#)
- [Анализ EDPB по соотношению норм GDPR и ePR](#)

Текущая редакция проекта ePrivacyRegulation, предложенная со стороны Совета ЕС под председательством Финляндии, была [отклонена](#) 22.11.2019 комитетом постоянных представителей Совета Европейского союза (the Permanent Representatives Committee of the Council of the European Union - COREPER).



[Proposal 2020/0340 \(COD\) on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC](#) - проект Директивы о представительских действиях по защите коллективных интересов потребителей в ЕС. Проект предусматривает, что все государства-члены ЕС должны ввести в действие по крайней мере один эффективный процессуальный механизм, который позволяет квалифицированным субъектам (например, потребительским организациям или государственным органам) подавать иски в суд с целью судебного запрета (прекращения действия или запрета) или возмещения (компенсации). Это касается, в том числе, защиты интересов субъектов персональных данных.

Полезные ссылки:

- [Текущий статус рассмотрения проекта](#)
- [Общее описание целей, задач, структуры и содержания проекта](#)



Brussels, 25.11.2020
COM(2020) 767 final
2020/0340 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European data governance
(Data Governance Act)

(Text with EEA relevance)

{SEC(2020) 405 final} - {SWD(2020) 295 final} - {SWD(2020) 296 final}

[Proposal 2020/0340 \(COD\) on European data governance \(Data Governance Act\)](#) - проект Регламента об управлении данными в ЕС, опубликованный 25.11.2020. По расчетам Европейской Комиссии, объем данных, генерируемых государственными органами, предприятиями и гражданами, постоянно растет. Ожидается, что в период с 2018 по 2025 год он увеличится в пять раз. Новый Регламент позволит использовать эти данные на благо общества, граждан и компаний.

Полезные ссылки:

- [Текущий статус рассмотрения проекта](#)
- [Общее описание целей, задач, структуры и содержания проекта](#)



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.

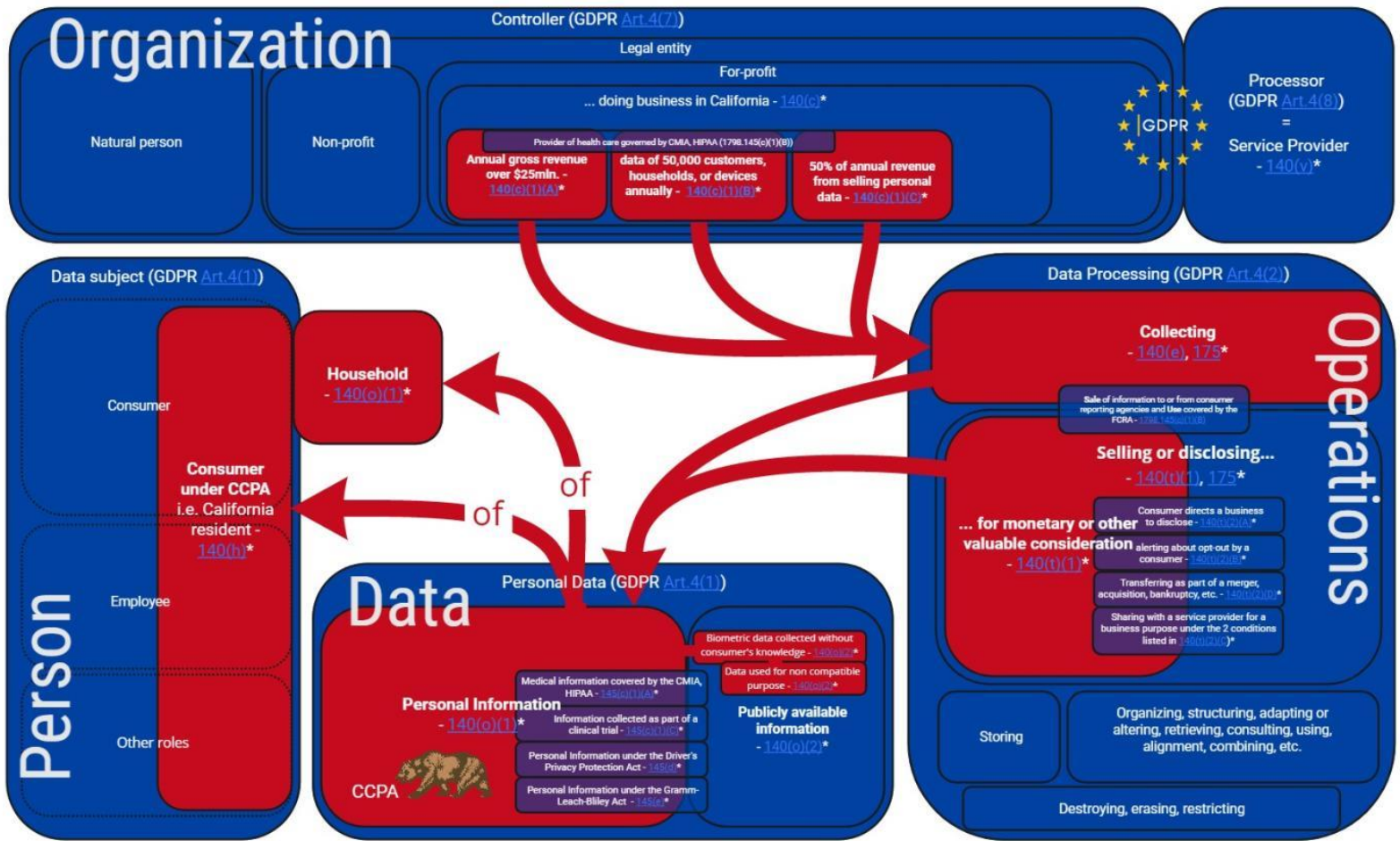
Новый закон штата Калифорнии во многом похож на GDPR, но идет дальше и позволяет потребителям отказаться от ранее предоставленного согласия на обработку своих персональных данных, при этом обязывая провайдеров онлайн-сервисов и социальных сетей продолжать оказывать услуги в адрес таких лиц.

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.](#)

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.com/en/person/siarhei-varankevich/

© Siarhei Varankevich CIPP/E, CIPM, MBA. 2020



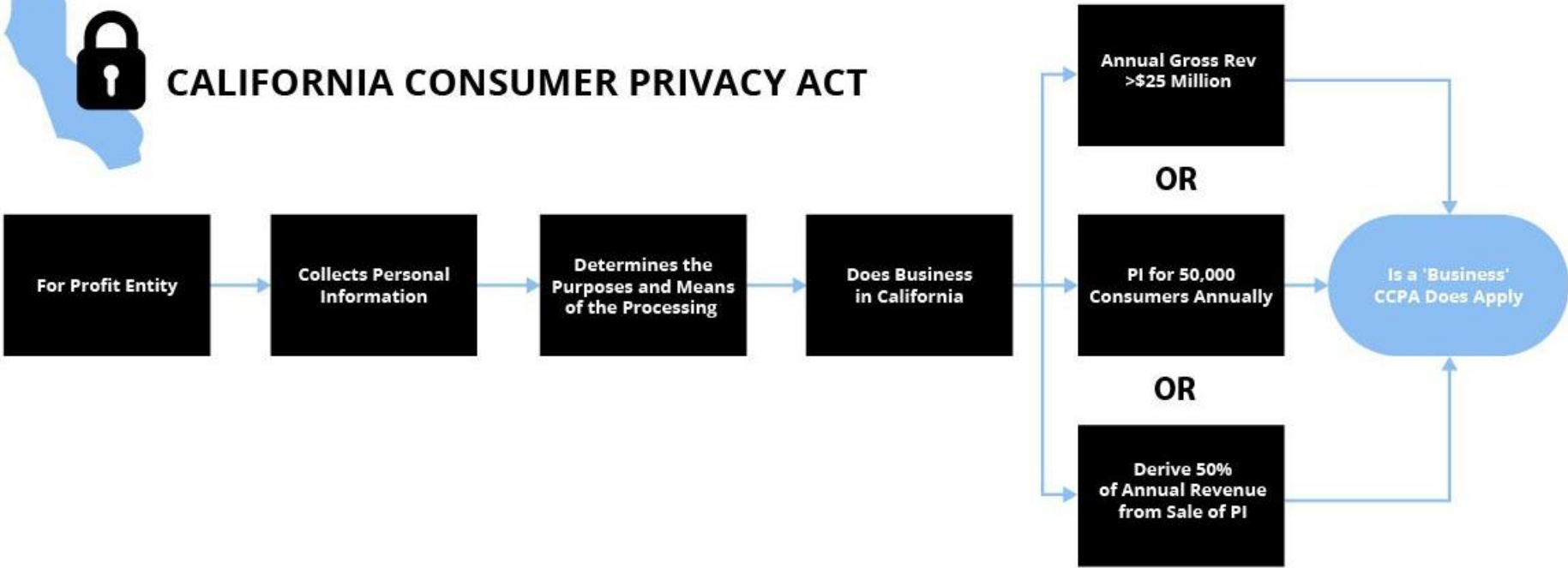
HOW TO READ THE DIAGRAM

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.



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.

NTIA Seeks Comment on New Approach to Consumer Data Privacy

Topics: [Internet Policy](#) [Internet Policy Task Force](#) [Privacy](#)

FOR IMMEDIATE RELEASE:

September 25, 2018

Today, the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) issued a [Request for Comments](#) on a proposed approach to consumer data privacy designed to provide high levels of protection for individuals, while giving organizations legal clarity and the flexibility to innovate.

The Request for Comments is part of a transparent process to modernize U.S. data privacy policy for the 21st century. In parallel efforts, the Commerce Department's National Institute of Standards and Technology is developing a voluntary privacy framework to help organizations manage risk; and the International Trade Administration is working to increase global regulatory harmony.

The Trump Administration's proposed approach focuses on the desired outcomes of organizational practices, rather than dictating what those practices should be. With the goal of building better privacy protections, NTIA is seeking comment on the following outcomes:

1. Organizations should be **transparent** about how they collect, use, share, and store users' personal information.
2. Users should be able to exercise **control** over the personal information they provide to organizations.
3. The collection, use, storage and sharing of personal data should be **reasonably minimized** in a manner proportional to the scope of privacy risks.
4. Organizations should employ **security** safeguards to protect the data that they collect, store, use, or share.
5. Users should be able to reasonably **access and correct** personal data they have provided.
6. Organizations should take steps to **manage the risk** of disclosure or harmful uses of personal data.
7. Organizations should be **accountable** for the use of personal data that has been collected, maintained or used by its systems.

U.S. Department of Commerce's National Telecommunications and Information Administration

Национальное управление по телекоммуникациям и информации (NTIA) Министерства торговли США опубликовало запрос о получении комментариев от всех сторон, заинтересованных в обсуждении общедофедерального подхода США в области обеспечения приватности персональных данных потребителей товаров, работ и услуг.

Также уже предложены следующие законопроекты:

- [Social Media Privacy Protection and Consumer Rights Act \(23.04.2018\)](#)
- [The Customer Online Notification for Stopping Edge-provider Network Transgressions Act \(10.04.2018\)](#)
- [Email Privacy Act \(27.07.2017\)](#)
- [Online Privacy Act \(11.07.2017\)](#)



MWC 2019 BEST PRODUCTS REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

POLITICS

At hearing on federal data-privacy law, debate flares over state rules

At a hearing before a US House of Representatives committee, witnesses lock horns over whether state regulations help or hinder data protection for consumers.

BY ALFRED NG | FEBRUARY 26, 2019 10:52 AM PST



A congressional hearing on data privacy looked at what lawmakers should include in a federal data-privacy bill.

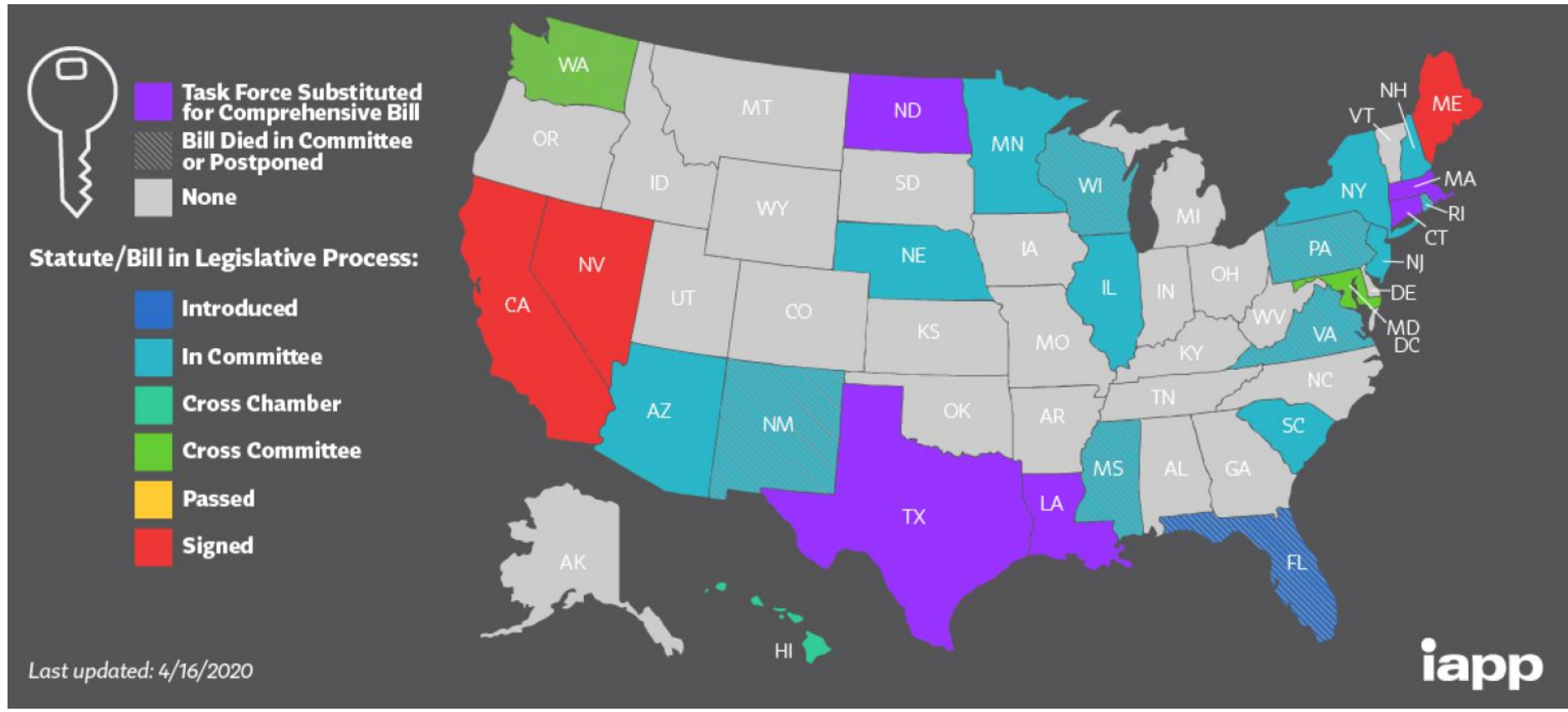
Tim Graham/Getty Images

There's a bipartisan call for a US data-privacy law, but there's a divide when it comes to balancing federal legislation with state rules.

On Tuesday the House Energy and Commerce Committee held its first hearing on data privacy, with a [Senate hearing](#) scheduled for Wednesday. Once just a blip on the political radar, data privacy has now set off a roaring alarm, as tech scandals have surfaced regularly over the last few years.

United States House of Representatives

Подкомитет по защите прав потребителей и коммерции Палаты представителей США согласился с необходимостью принятия нового федерального закона о конфиденциальности, но отклонил GDPR и ССРА в качестве модели регулирования для будущего федерального законодательства о конфиденциальности. Тем не менее, был достигнут консенсус в отношении того, что полное игнорирование регуляторной модели защиты персональных данных в ЕС и Калифорнии является контрпродуктивным.



Ситуация по законодательству о Privacy в США на 04.2020



State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	Consumer Rights				Business Obligations											
				Right of Access	Right of Rectification	Right of Deletion	Right of Restriction	Right of Portability	Right of Opt-Out	Right Against Automated Decision Making	Private Right of Action (s = security only)	Strict Age Opt-in for Prohibition on Sale of Information	Notice/Transparency Requirement	Data Breach Notification	Risk Assessments	Prohibition on Discrimination (exercising rights)	Purpose Limitation	Processing Limitation	Fiduciary Duty
Arizona		SB 1614		x	x	x		16											
Arizona ¹		HB 2729		x	x	x	x	x											
California		AB 375/SB 1121	California Consumer Privacy Act	x	x	x	x	s 16	x										
Connecticut		RB 1108		Task force substituted for comprehensive bill.															
Florida		H 963								x									
Hawaii ¹¹		HB 2572								p									
Hawaii		HCR 225		Task force substituted for comprehensive bill.															
Hawaii		SB 418		x	x	x	x			16	x								
Illinois		SB 2263	Data Privacy Act	x	x	x	x				x	x							
Illinois		SB 2330	Illinois Data Transparency and Privacy Act	x	x	x	x			s	x	x							
Illinois		HB 5603	Consumer Privacy Act	x	x	x	x			s 16	x								
Louisiana		HR 249		Task force substituted for comprehensive bill.															
Maine ¹¹		LD 946	An Act to Protect the Privacy of Online Consumer Information			x	in				x								
Maryland		HB 249									x								
Maryland ¹²		HB 784	Online Consumer Protection Act	x	x	x	x				x								
Maryland ¹³		HB 1656		x	x	x	x			s 16	x								
Massachusetts		S 120		Study order issued.															
Minnesota		HF 3936	Minnesota Consumer Data Privacy Act	x	x	x	x				x	x	x	x					
Mississippi		HB 1253	Mississippi Consumer Privacy Act	x	x	x	x			s 16	x								
Nebraska		LB 746	Nebraska Consumer Data Privacy Act	x	x					16	x								
Nevada		SB 220/Ch. 603A									x								
New Hampshire ¹⁴		HB 1236									x								
New Hampshire		HB 1680		x	x	x	x			s	x								
New Jersey		A 2188		x							x								
New Jersey ¹⁵		A3255		x	x	x	in				x								
New Jersey		S 2834									x								
New Mexico		SB 176	Consumer Information Privacy Act	x	x	x	x			s 18	x								
New York		S 224	Right to Know Act								x								
New York		S 5642	New York Privacy Act	x	x	x	x	x	x		x	x							x
North Dakota		HB 1485		Task force substituted for comprehensive bill.															
Pennsylvania		HB 1049	Consumer Data Privacy Act	x	x					s 16	x								
Rhode Island		S 0234	Consumer Privacy Protection Act	x	x	x	x			s 16	x								
South Carolina ¹⁶		H 4812	South Carolina Biometric Data Privacy Act	x	x					16	x	x	x	x					
Texas		HB 4390	Texas Privacy Protection Act	Task force substituted for comprehensive bill.															
Texas		HB 4518	Texas Consumer Privacy Act	x	x	x	x			16	x								
Virginia		HB 473	Virginia Privacy Act	x	x	x	x				x								
Washington		SB 6281	Washington Privacy Act	x	x	x	x				x	x	x	x					
Wisconsin		AB 870	Wisconsin Data Privacy Act (i)	x							x	x							
Wisconsin		AB 871	Wisconsin Data Privacy Act (ii)								x								
Wisconsin		AB 872	Wisconsin Data Privacy Act (iii)								x								x

In Session: all above states

Introduced
In Committee
Crossed Chamber
Cross Committee
Passed
Signed

Bold - passed law
Strikethrough - bill died in committee or postponed

s - private right of action for security violations only
in - opt-in consent requirement
p - prohibition without consent

Модернизация Конвенции 108 и ее влияние на регулирование в РФ





European Treaty Series – No. 108
Série des Traités européens - n° 108

Convention for the Protection of Individuals
with regard to Automatic Processing
of Personal Data
as it will be amended
by its Protocol CETS No. [223]

Convention pour la protection des personnes
à l'égard du traitement automatisé
des données à caractère personnel
telle qu'elle sera amendée
par son Protocole STCE n° [223]

Strasbourg, 28.I.1981

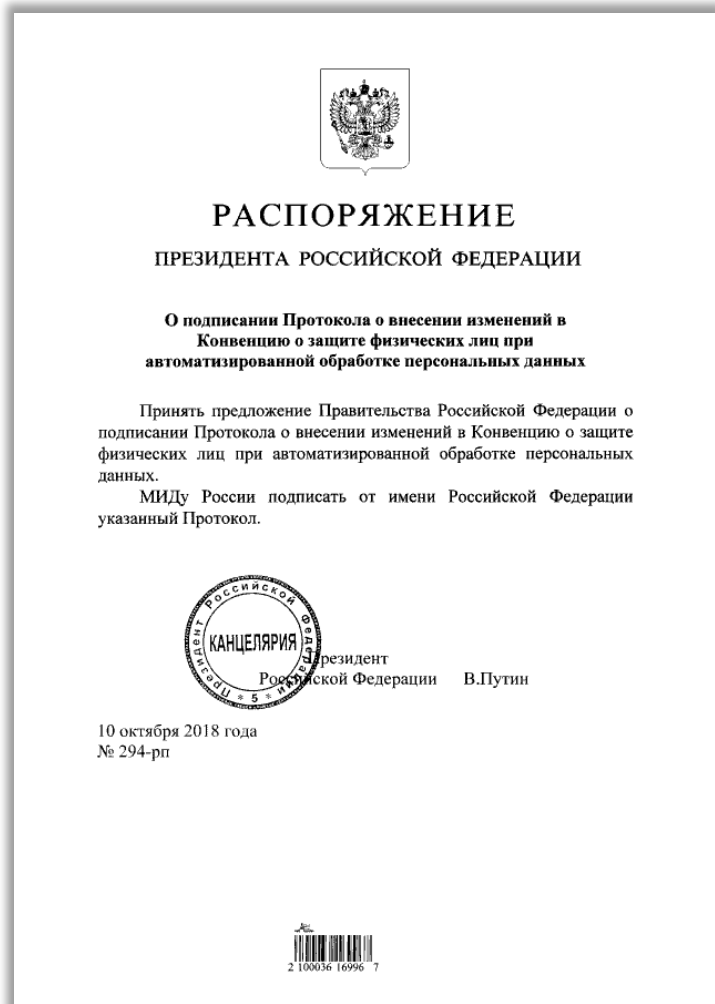
На 128-ой сессии Комитета министров Совета Европы, состоявшейся 18.05.2018, был принят Протокол СДСЕ № 223, вносящий существенные изменения в Конвенцию и превращающие ее в «**Конвенцию 108+**», в том числе, и в сфере гармонизации многих положений Конвенции с нормами GDPR.

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](#)

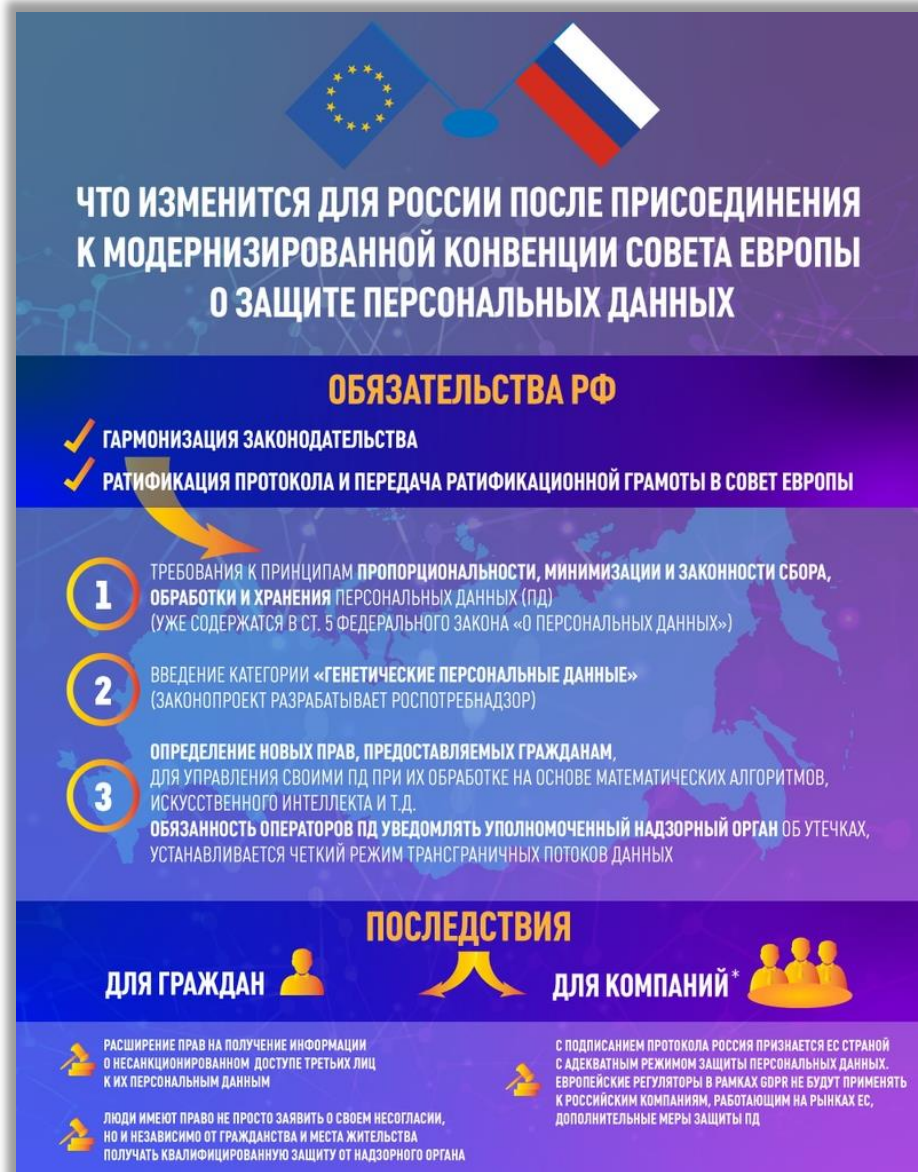


Согласно поручению Президента РФ, постоянный представитель России при Совете Европы Иван Солтановский от имени России в Страсбурге 10.10.2018 подписал Протокол СДСЕ № 223 об изменениях в европейскую Конвенцию о защите физических лиц при автоматизированной обработке персональных данных № 108.

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...

Начиная с 2020 года Россию ожидает крупнейшая за десятилетие реформа законодательства о персональных данных, которая кардинально изменит существующие правила.



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» (ЗАКОНОПРОЕКТ 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

-  РАСШИРЕНИЕ ПРАВ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ О НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ ТРЕТЬИХ ЛИЦ К ИХ ПЕРСОНАЛЬНЫМ ДАННЫМ
-  ЛЮДИ ИМЕЮТ ПРАВО НЕ ПРОСТО ЗАЯВИТЬ О СВОЕМ НЕСОГЛАСИИ, НО И НЕЗАВИСИМО ОТ ГРАЖДАНСТВА И МЕСТА ЖИТЕЛЬСТВА ПОЛУЧАТЬ КВАЛИФИЦИРОВАННУЮ ЗАЩИТУ ОТ НАДЗОРНОГО ОРГАНА

ДЛЯ КОМПАНИЙ*

-  С ПОДПИСАНИЕМ ПРОТОКОЛА РОССИЯ ПРИЗНАЕТСЯ ЕС СТРАНОЙ С АДЕКВАТНЫМ РЕЖИМОМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ. ЕВРОПЕЙСКИЕ РЕГУЛЯТОРЫ В РАМКАХ GDPR НЕ БУДУТ ПРИМЕНЯТЬ К РОССИЙСКИМ КОМПАНИЯМ, РАБОТАЮЩИМ НА РЫНКАХ ЕС, ДОПОЛНИТЕЛЬНЫЕ МЕРЫ ЗАЩИТЫ ПД

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.

проект

РОССИЙСКАЯ ФЕДЕРАЦИЯ**ФЕДЕРАЛЬНЫЙ ЗАКОН****О ратификации Протокола о внесении изменений
в Конвенцию Совета Европы о защите физических лиц
при автоматизированной обработке персональных данных**

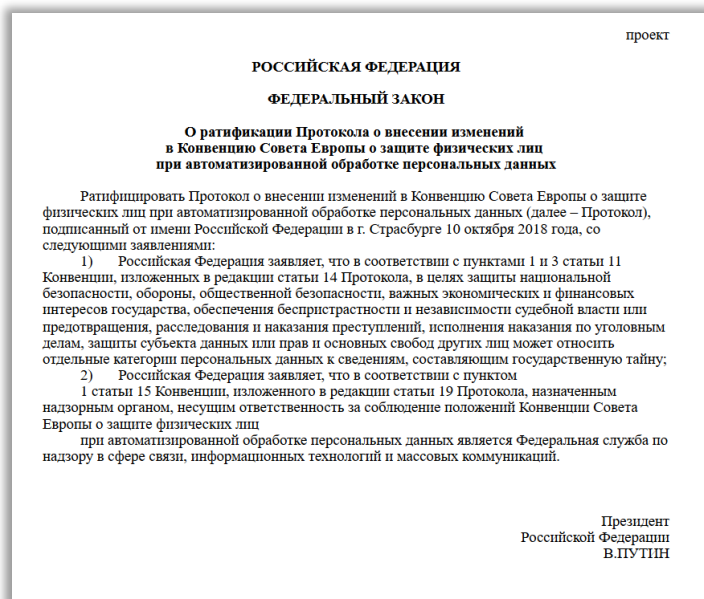
Ратифицировать Протокол о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (далее – Протокол), подписанный от имени Российской Федерации в г. Страсбурге 10 октября 2018 года, со следующими заявлениями:

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».



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.**

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 инструментарий 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/ru/press/2019/07/02).

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 инструментарий Конвенции носит универсальный характер и полностью регулирует процедуру трансграничного исполнения вынесенных судебных решений.

Regulation	GDPR	Russia	Ukraine	Belarus	Kazakhstan	Georgia
Right of access by the data subject	✓	✓	✓	✗	✓	✓
Right to be forgotten	✓	✓	✓	✗	✓	✓
Right to data portability	✓	✗	✗	✗	✗	✗
Right to withdraw consent	✓	✓	✓	✗	✓	✓
Right to rectification	✓	✓	✓	✗	✓	✓
Personal data breach notification	✓	✗	✗	✗	✗	✗
Purpose limitation and data minimization	✓	✓	✓	✗	✓	✓
Cross-border data transfer limitations	✓	✓	✓	✓	✓	✓
Data localization requirements	✗	✓	✗	!	✓	✗
Extraterritorial effect	✓	!	✗	✗	✗	!



Этот смелый эскиз называется «Заяц, начитавшийся Байрона GDPR, в бурную ночь на утёсе вглядывается в бушующую бездну».

Мел, стенка, 1X1.

Благодарю за ваше внимание



Алексей Мунтян

***Соучредитель Ассоциации профессионалов в области
приватности (rppa.ru)***

Data Privacy Manager в крупном международном холдинге

***Член Совета ТПП РФ по развитию антикоррупционного
комплаенса и деловой этики***

+7 (903) 762-64-15

muntyan.alexey@gmail.com

facebook.com/alexey.muntyan

linkedin.com/in/alexey-muntyan