Глобальные и европейские практики локализации данных и ограничения их трансграничного оборота

Редакция от 2022.04.08

2 Динамика эволюции требований локализации данных в 2017-2021гг.

1. В XXI веке требования локализации данных активно эволюционировали в сторону увеличения как диапазона охватываемых данных, так количества стран.
2. Число стран, которые ввели требования локализации данных, почти удвоилось с 35 в 2017 году до 62 в 2021 году.
3. Общее количество действующих требований локализации данных (как формальных, так и фактических) увеличилось более чем вдвое с 67 в 2017 году до 144 в 2021 году.
4. На конец 2021 года на планете в стадии рассмотрения находится 38 новых требований локализации данных.
5. Китай (29), Индия (12), Россия (9) и Турция (7) являются мировыми лидерами по количеству требований локализации данных и их охвату.

3 Наиболее популярная аргументация в пользу локализации данных

Аргументация политиков и иных заинтересованных лиц в необходимости локализации данных демонстрирует постоянную эволюцию.

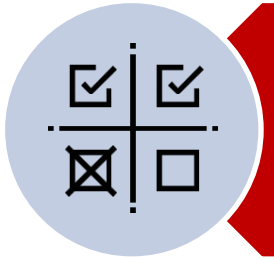
Многие ранее непреднамеренно поддерживали локализацию, поскольку не понимали, как международные компании управляют данными на глобальном уровне, соблюдая при этом местные законы.

Однако все больше политиков открыто поддерживают локализацию как форму протекционизма. Например, во Франции, Индии и Южной Корее творчески подходят к использованию произвольного и непрозрачного лицензирования, сертификации и других нормативных ограничений для создания условий вынужденной локализации данных (и выдавливания из национального рынка иностранных компаний и продуктов).

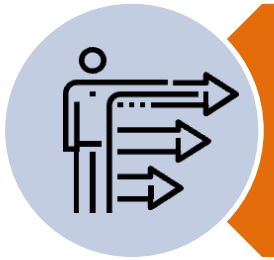
Основные мотивы, используемые для обоснования политики локализации данных:

1. обеспечение конфиденциальности и кибербезопасности (*например, Индия*);
2. цифровой протекционизм и суверенитет данных (*например, ЕС*);
3. контроль цифрового пространства (*например, Китай*);
4. содействие местным правоохранительным и надзорным органам (*например, Турция*);
5. геополитические риски и финансовые санкции (*например, Россия*).

4 Основные виды ограничений трансграничного оборота данных



Формальное ограничение передачи определенных типов данных за пределы границ государства



Фактическое ограничение трансграничной передачи путем создания условий, затрудняющих такую передачу – она становится сложной, дорогостоящей и нестабильной)

Ограничение оборота данных, определяемых в широких и расплывчатых категориях: «конфиденциальные», «важные», «ключевые» или «относящиеся к национальной безопасности»

Ранжирование типов локализации по степени ограничения свободы оборота данных

Локальная репликация данных (*Local data mirroring*). Необходимо хранить копию данных локально, но передача данных за пределы страны разрешена. В некоторых случаях требуется соблюдение последовательности обработки данных в виде их локального сбора и/или актуализации.

Локальное хранение данных (*Explicit local data storage*). Данные должны физически находится в стране их происхождения. В некоторых случаях допускается трансграничный доступ к данным для их обработки, но с условием локализации результатов обработки данных в стране их происхождения.

Вынужденное локальное хранение и обработка данных (*De facto local storage and processing*). Локальное хранение данных является вынужденным из-за строгих требований к трансграничной передаче (например, необходимость получения предварительного одобрения на передачу) и правовой неопределенности в отношении передачи данных, что в сочетании со значительными штрафами и произвольной надзорной практикой создает неприемлемый регуляторный риск.

Локальное хранение и обработка данных (*Explicit local data storage and processing*). Государство явно запрещает трансграничную передачу данных.

Дискриминационное локальное хранение и обработка данных (*Discriminatory local storage and data processing*). Государство применяет дискриминационные лицензирование, сертификацию и другие нормативные ограничения, требующие локального хранения данных и полностью исключающие иностранные организации из процессов локального управления и обработки данных.

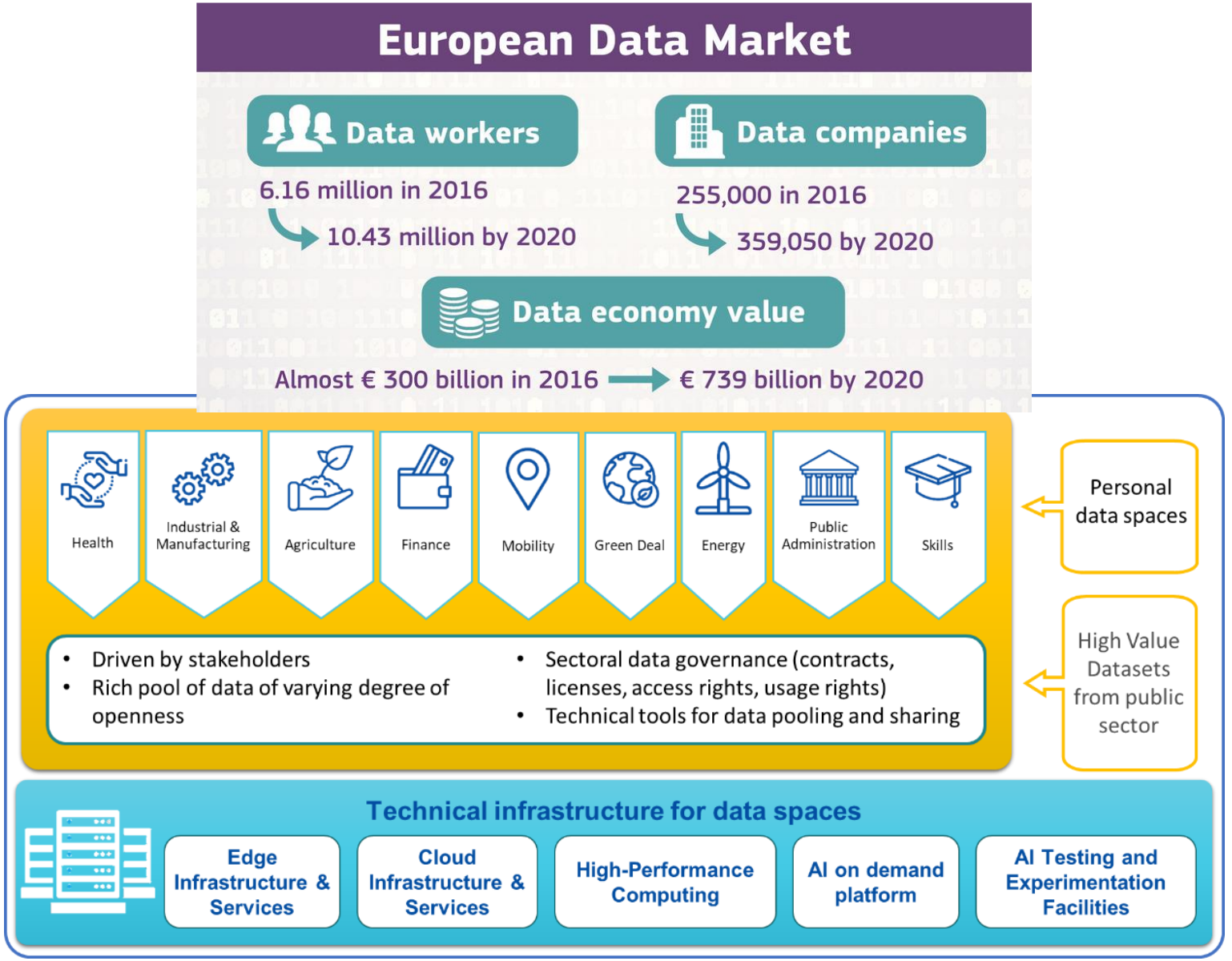
6 Категории локализуемых данных: практика крупных стран

Страны / Категории данных														
Персональные	●	●				●	●	●	●	●	●	●	●	●
Финансовые, налоговые, банковские	●		●		●		●	●		●	●	●		
Платежные	●							●			●	●		●
Геолокационные								●		●	●	●		
Медицинские, генетические					●						●	●		
Государственные	●	●		●		●				●		●	●	
Телекоммуникационные	●		●			●		●			●	●		
Публично-облачные	●						●		●					
Коммерческие, технические											●	●		●

7 EU Digital Single Market Strategy

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

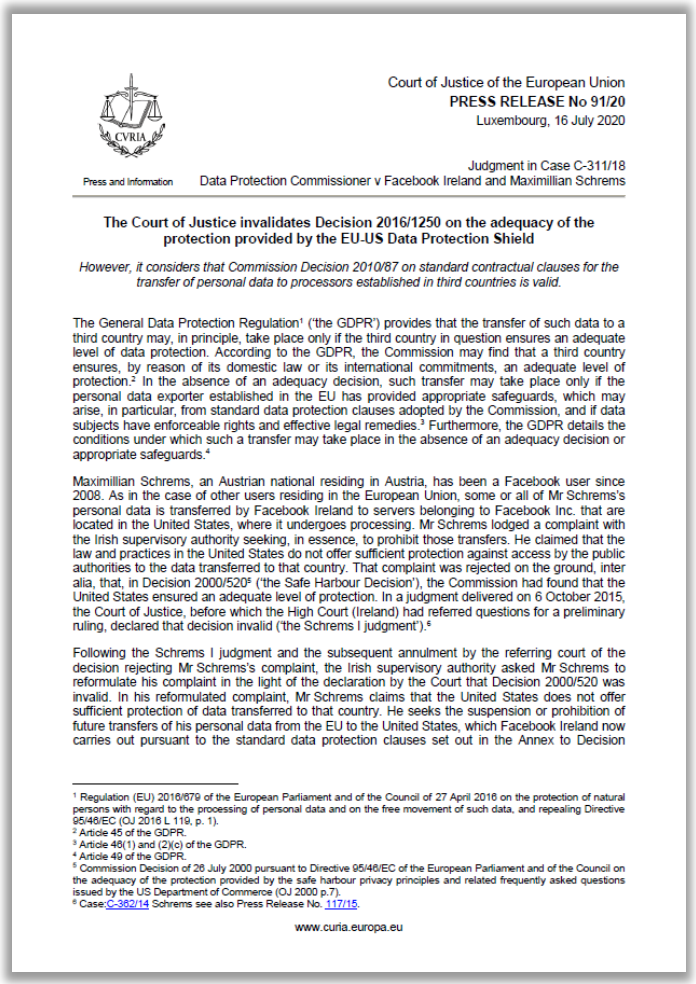
European Data Economy Strategy 2018



https://digital-strategy.ec.europa.eu/en/library/elements-european-data-economy-strategy-2018

https://europeansting.com/2021/07/07/parliament-adopts-temporary-rules-to-detect-child-sexual-abuse-online/

CJEU о недействительности Privacy Shield и об уточнении в отношении стандартных договорных условий (SCC-P)



Court of Justice of the European Union
PRESS RELEASE No 91/20
Luxembourg, 16 July 2020

Press and Information

Judgment in Case C-311/18
Data Protection Commissioner v Facebook Ireland and Maximillian Schrems

The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield

However, it considers that Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries is valid.

The General Data Protection Regulation[1] ('the GDPR') provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection.[2] In the absence of an adequacy decision, such transfer may take place only if the personal data exporter established in the EU has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies.[3] Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards.[4]

Maximillian Schrems, an Austrian national residing in Austria, has been a Facebook user since 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data is transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence, to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520[5] ('the Safe Harbour Decision'), the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court of Justice, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the Schrems I judgment').[6]

Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of future transfers of his personal data from the EU to the United States, which Facebook Ireland now carries out pursuant to the standard data protection clauses set out in the Annex to Decision

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1).
[2] Article 45 of the GDPR.
[3] Article 46(1) and (2)(c) of the GDPR.
[4] Article 49 of the GDPR.
[5] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 p.7).
[6] Case C-362/14 Schrems see also Press Release No. 117/15.

www.curia.europa.eu

Court of Justice of the European Union

Judgment in Case C-673/17
Data Protection Commissioner v
Facebook Ireland Limited, Maximillian Schrems

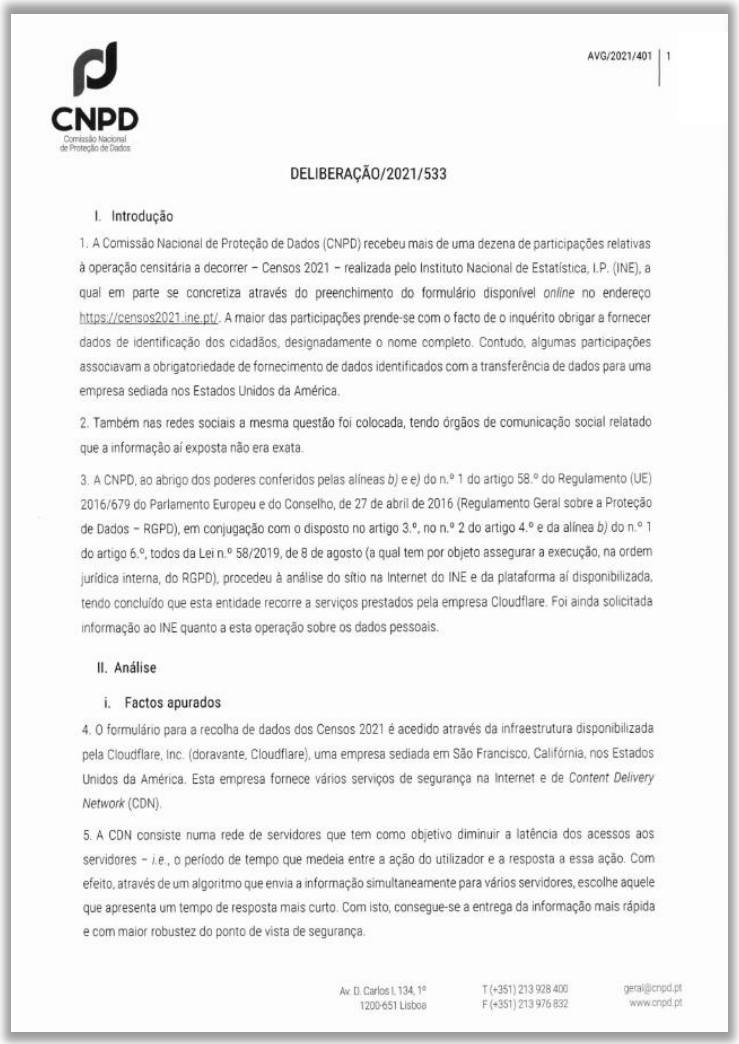
Суд постановил, что:

1. Privacy Shield признается недействительным в связи с недостаточной защищенностью персональных данных от передачи операторами социальных сетей американским спецслужбам. В решении суда говорится, что данное соглашение создает условия для нарушения фундаментальных прав европейских граждан. В нем подчеркивается, что в США доступ государственных структур к подобной информации ограничен в гораздо меньшей степени, чем в странах ЕС.

2. SCC-P (Standard Contractual Clauses Controller-to-Processor) не должны быть признаны недействительными, но экспортеры и импортеры персональных данных из ЕС должны предпринимать необходимые и достаточные меры для обеспечения соблюдения SCC-P. В частности, экспортер данных при содействии импортера должен оценить адекватность защиты прав субъектов данных в юрисдикции импортера данных, а также способен ли импортер данных выполнять все требования SCC-P. Кроме того, надзорные органы ЕС (DPA) обязаны приостановить или запретить передачу данных в третью страну, если они считают принципиально невозможным обеспечение требуемого законодательством ЕС уровня защиты прав субъектов данных, даже при наличии действующего SCC между экспортером и импортером.

https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

Португальский надзорный орган запретил трансграничную передачу данных в адрес компании Cloudflare



CNPD
Comissão Nacional de Proteção de Dados

AVG/2021/401 | 1

DELIBERAÇÃO/2021/533

I. Introdução

1. A Comissão Nacional de Proteção de Dados (CNPD) recebeu mais de uma dezena de participações relativas à operação censitária a decorrer – Censos 2021 – realizada pelo Instituto Nacional de Estatística, I.P. (INE), a qual em parte se concretiza através do preenchimento do formulário disponível *online* no endereço https://censos2021.ine.pt/. A maior das participações prende-se com o facto de o inquérito obrigar a fornecer dados de identificação dos cidadãos, designadamente o nome completo. Contudo, algumas participações associavam a obrigatoriedade de fornecimento de dados identificados com a transferência de dados para uma empresa sediada nos Estados Unidos da América.

2. Também nas redes sociais a mesma questão foi colocada, tendo órgãos de comunicação social relatado que a informação aí exposta não era exata.

3. A CNPD, ao abrigo dos poderes conferidos pelas alíneas *b)* e *e)* do n.º 1 do artigo 58.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º e da alínea *b)* do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto (a qual tem por objeto assegurar a execução, na ordem jurídica interna, do RGPD), procedeu à análise do sítio na Internet do INE e da plataforma aí disponibilizada, tendo concluído que esta entidade recorre a serviços prestados pela empresa Cloudflare. Foi ainda solicitada informação ao INE quanto a esta operação sobre os dados pessoais.

II. Análise

i. Factos apurados

4. O formulário para a recolha de dados dos Censos 2021 é acedido através da infraestrutura disponibilizada pela Cloudflare, Inc. (doravante, Cloudflare), uma empresa sediada em São Francisco, Califórnia, nos Estados Unidos da América. Esta empresa fornece vários serviços de segurança na Internet e de *Content Delivery Network* (CDN).

5. A CDN consiste numa rede de servidores que tem como objetivo diminuir a latência dos acessos aos servidores – *i.e.*, o período de tempo que medeia entre a ação do utilizador e a resposta a essa ação. Com efeito, através de um algoritmo que envia a informação simultaneamente para vários servidores, escolhe aquele que apresenta um tempo de resposta mais curto. Com isto, consegue-se a entrega da informação mais rápida e com maior robustez do ponto de vista de segurança.

Av. D. Carlos I, 134, 1º
1200-651 Lisboa
T (+351) 213 928 400
F (+351) 213 976 832
geral@cnpd.pt
www.cnpd.pt

27.04.2021 португальский орган по защите данных (CNPD) издал предписание, требующее от Национального статистического института (INE) приостановить в течение 12 часов любую трансграничную передачу персональных данных, в частности данных переписи 2021 года, в США или другие третьи страны без адекватного уровня защиты в соответствии с решением CJEU Schrems II. В решении отмечается, что после жалоб на условия сбора данных для переписи 2021 года CNPD провела расследование и пришла к выводу, что INE привлекла компанию Cloudflare, Inc. в качестве сервис-провайдера обработки данных.

Cloudflare является калифорнийской компанией и напрямую подчиняется законодательству США о слежке в целях обеспечения национальной безопасности, которое налагает юридическое обязательство предоставлять властям США неограниченный доступ к любым данным, находящимся во распоряжении компании, без права уведомления о таком доступе других лиц (субъектов данных).

Регулятор также отметил, что передаваемые данные включали такие чувствительные категории как сведения о религиозных убеждениях и о состоянии здоровья. Поэтому CNPD принял решение, что передача таких данных в США или любую другую третью страну без надлежащей защиты должна быть приостановлена.

https://www.cnpd.pt/comunicacao-publica/noticias/censos-2021-cnpd-suspende-fluxos-para-os-eua/

Баварский надзорный орган запретил трансграничную передачу данных в адрес компании Mailchimp

edpb
European Data Protection Board

MENU

Bavarian DPA (BayLDA) calls for German company to cease the use of 'Mailchimp' tool

Tuesday, 30 March, 2021 DE

The "ruling" presented in the "Standard" concerns a remedy procedure concluded without formal supervisory measures regarding a complaint by a data subject, in which the controller (an individual company) that had used Mailchimp had, after our request for comments and detailed information on the consequences of the Schrems II- decision, announced that it had now refrained from using Mailchimp.

Our final notice to the complainant, which apparently formed the basis of the publication and was sent in mid-March, had the following wording in extracts and translated informally:

"... We are referring to your data protection complaint against .... concerning the use of "Mailchimp". As a result of our intervention, the company has informed us that it had used Mailchimp twice to send newsletters. As a result of our intervention, the company has now informed us that it will no longer use Mailchimp with immediate effect.

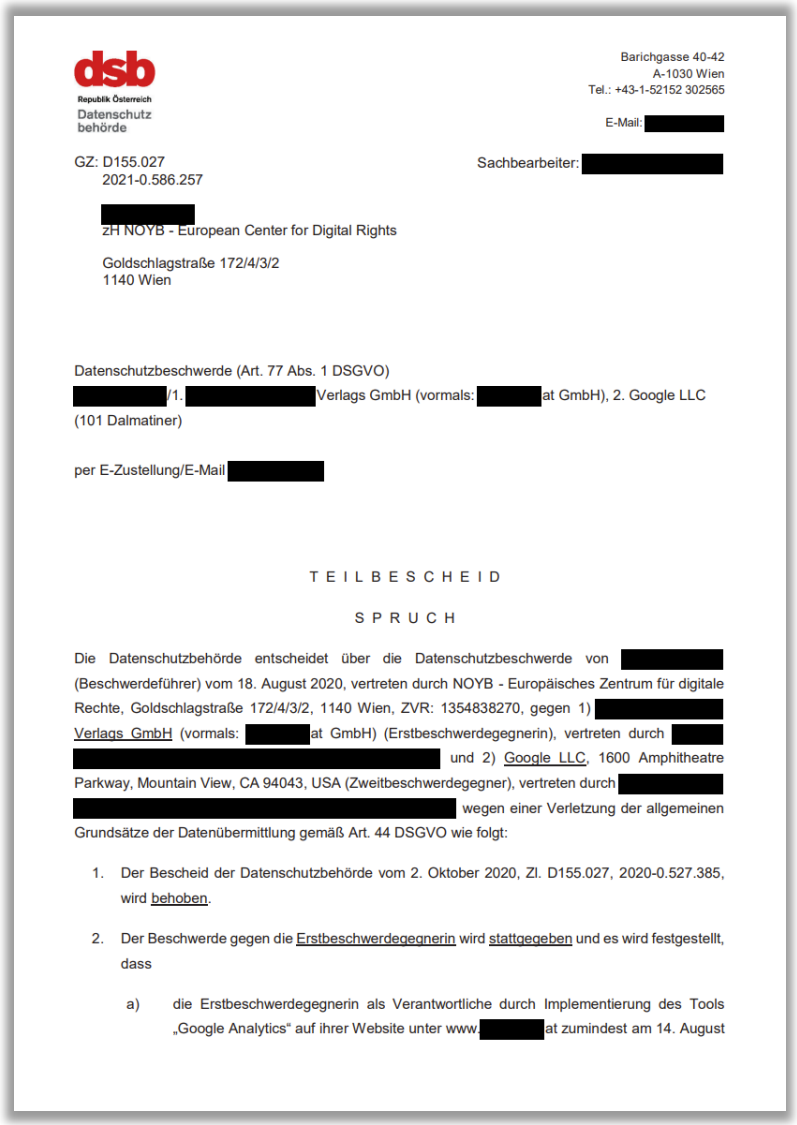
The company also informed us that it had only transmitted email addresses to Mailchimp in the context of the above-mentioned use. It also mentioned that the recommendations of the European Data Protection Board on the so-called Supplementary Measures for transfers of personal data to third countries are not yet available in a final version, but are still

15.03.2021 баварское DPA завершило расследование по жалобе на неназванную немецкую компанию, которая дважды использовала американскую платформу электронного маркетинга Mailchimp для информационной рассылки своим клиентам. Хотя компания предоставила Mailchimp адреса электронной почты в соответствии с SCC, DPA Баварии сочло передачу незаконной, поскольку компания не проверила, потребуются ли «дополнительные меры» в соответствии с решением CJEU Schrems II для обеспечения адекватной защиты данных.

Баварский надзорный орган принял свое решение исходя из наличия «признаков того, что Mailchimp в принципе может получать запросы на доступ к данным со стороны американских спецслужб», и, следовательно, трансграничная передача данных из ЕС может быть дозволена только при условии принятия экспортёром и импортёром данных дополнительных мер защиты, которые будут достаточными для устранения потенциальной угрозы неправомерного доступа к данным. В конце концов, расследование было прекращено по причине прекращения использования сервиса Mailchimp со стороны немецкой компании.

Подробнее: https://edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool_en
https://www.project-disco.org/european-union/040621-the-monkeys-pause-mailchimp-data-transfers-halted-in-german-schrems-ii-inquiry/

Австрийский DSB решил, что использование Google Analytics нарушает решение CJEU "Schrems II"



dsb
Republik Österreich
Datenschutz behörde

Barichgasse 40-42
A-1030 Wien
Tel.: +43-1-52152 302565
E-Mail: [redacted]

GZ: D155.027
2021-0.586.257

Sachbearbeiter: [redacted]

[redacted]
zH NOYB - European Center for Digital Rights

Goldschlagstraße 172/4/3/2
1140 Wien

Datenschutzbeschwerde (Art. 77 Abs. 1 DSGVO)
[redacted]/1. [redacted] Verlags GmbH (vormals: [redacted] at GmbH), 2. Google LLC
(101 Dalmatiner)

per E-Zustellung/E-Mail [redacted]

T E I L B E S C H E I D

S P R U C H

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von [redacted] (Beschwerdeführer) vom 18. August 2020, vertreten durch NOYB - Europäisches Zentrum für digitale Rechte, Goldschlagstraße 172/4/3/2, 1140 Wien, ZVR: 1354838270, gegen 1) [redacted] Verlags GmbH (vormals: [redacted] at GmbH) (Erstbeschwerdegegnerin), vertreten durch [redacted] und 2) Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Zweitbeschwerdegegner), vertreten durch [redacted] wegen einer Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO wie folgt:

1. Der Bescheid der Datenschutzbehörde vom 2. Oktober 2020, Zl. D155.027, 2020-0.527.385, wird behoben.

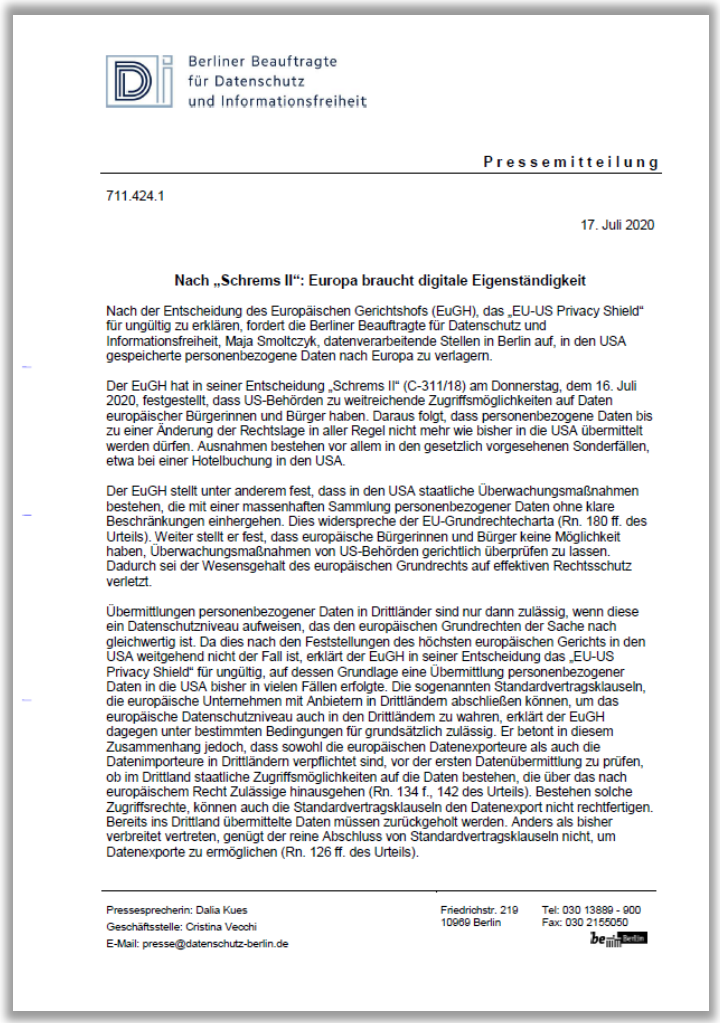
2. Der Beschwerde gegen die Erstbeschwerdegegnerin wird stattgegeben und es wird festgestellt, dass

   a) die Erstbeschwerdegegnerin als Verantwortliche durch Implementierung des Tools „Google Analytics“ auf ihrer Website unter www.[redacted] at zumindest am 14. August

13.01.2022 австрийский орган по защите данных («Datenschutzbehörde» или «DSB») принял новаторское решение по жалобе австрийской НКО NOYB о том, что постоянное использование Google Analytics нарушает GDPR. Это первое решение по 101 типовой жалобе, поданной NOYB после так называемого решения «Шремс II». В 2020 году Суд (CJEU) постановил, что использование американских провайдеров нарушает GDPR, поскольку законы США о слежке требуют, чтобы американские провайдеры, такие как Google или Facebook, предоставляли личные данные властям США. Аналогичные решения ожидаются и в других странах-членах ЕС.

https://www.cnpd.pt/comunicacao-publica/noticias/censos-2021-cnpd-suspende-fluxos-para-os-eua/
https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal

Локализация обработки персональных данных по-немецки



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
10969 Berlin
Tel: 030 13889 - 900
Fax: 030 2155050

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.

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf

Благодарю за ваше внимание

Алексей Мунтян

Основатель и CEO в компании Privacy Advocates

Соучредитель и член Правления в Russian Privacy Professionals Association - RPPA.ru

+7 (903) 762-64-15
t.me/prv_adv
muntyan.alexey@gmail.com
privacy-advocates.ru/bio.pdf
facebook.com/alexey.muntyan
linkedin.com/in/alexey-muntyan