

Рассмотрение механизмов и специфики применения Генерального регламента ЕС о защите данных (GDPR)

Алексей Мунтян

Редакция от 10.04.2020

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

2 Вместо предисловия…



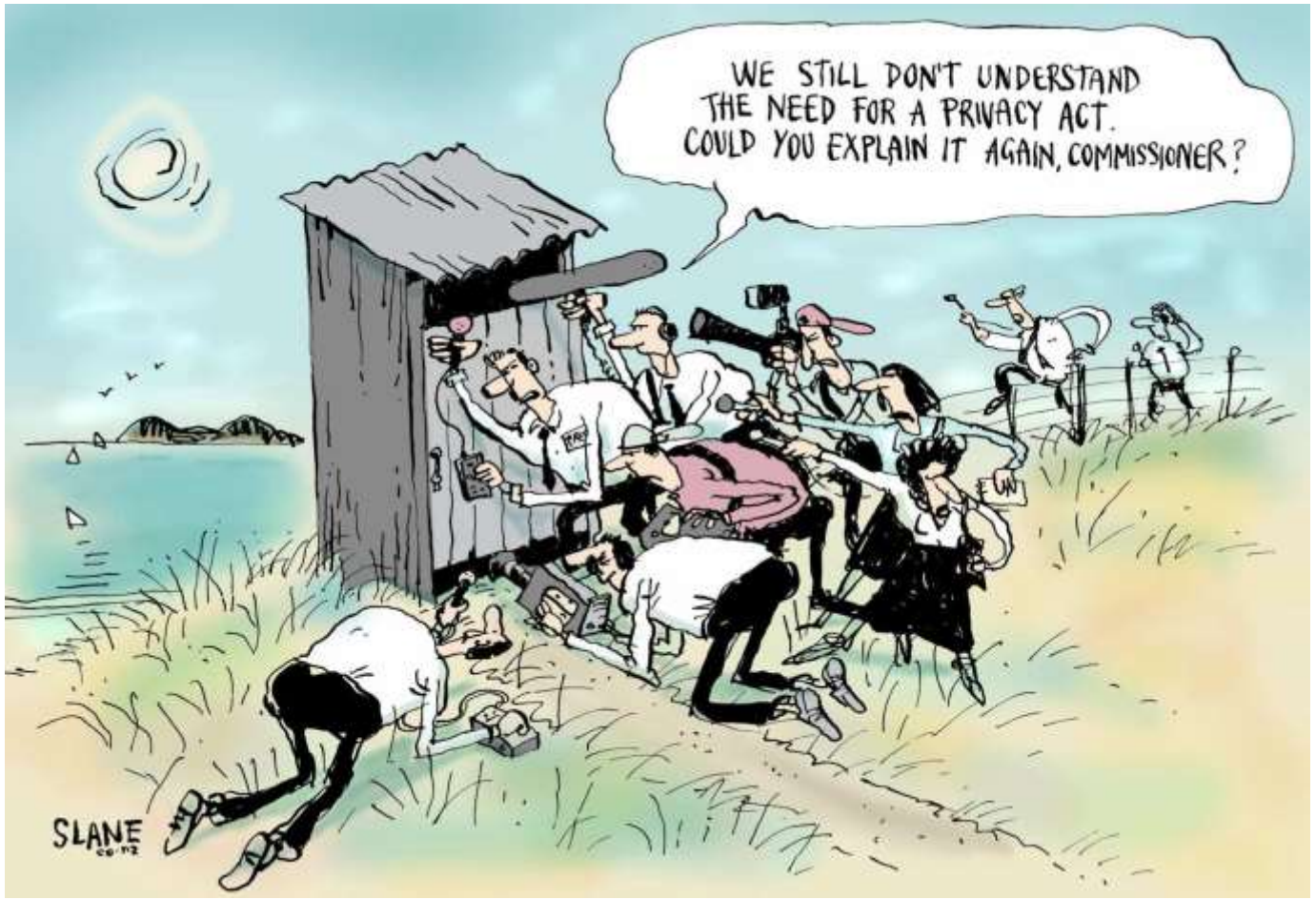
Этот смелый эскиз называется «Заяц, начитавшийся ~~Байрона~~ GDPR, в бурную ночь на утёсе вглядывается в бушующую бездну».

Мел, стенка, 1X1.

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 Officer
6. Legitimate Interests
7. Data Protection Impact Assessment
8. Управление Data Breach
9. Автоматизация Privacy и Data Protection
10. Взаимодействие с пользователями сайтов и приложений
11. Большие данные, искусственный интеллект и машинное обучение
12. Data Protection (Privacy) by Design and by Default
13. Records of Processing Activities
14. Защита персональных данных
15. Псевдонимизация и анонимизация
16. Международные стандарты
17. Правоприменительная практика
18. Штрафы - базы дел и аналитика
19. Штрафы - интересные кейсы
20. Иные санкции и меры принуждения
21. Судебная практика – базы решений и интересные ситуации
22. Влияние GDPR на бизнес
23. Итоги применения GDPR в 2018-2019 и дальнейшие перспективы
24. Законодательные инициативы о персональных данных в ЕС и США
25. Модернизация Конвенции 108 и ее влияние на регулирование в РФ

Обзор контекста принятия и механизмов GDPR



К оглавлению

Эволюция европейского законодательства о защите данных

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 (public sec.)

1973 First national privacy law: Data Act, Sweden

1981 (CoE) Convention 108

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

2013 (OECD) OECD Guidelines updated

2016 (EU) EU-US Privacy Shield approved

2018 (CoE) Convention 108 updated

2016 (EU) NIS Directive

2016 (EU) Law Enforcement Directive

2016 (EU) PNR Directive

20?? (EU) ePrivacy Regulation

Relevant context and data protection law

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

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



Mainframe



PC



Usenet









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



High profile data breaches and/or concerns



Edward Snowden disclosures about global surveillance



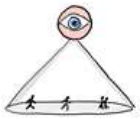
Max Schrems



Social Media Trends



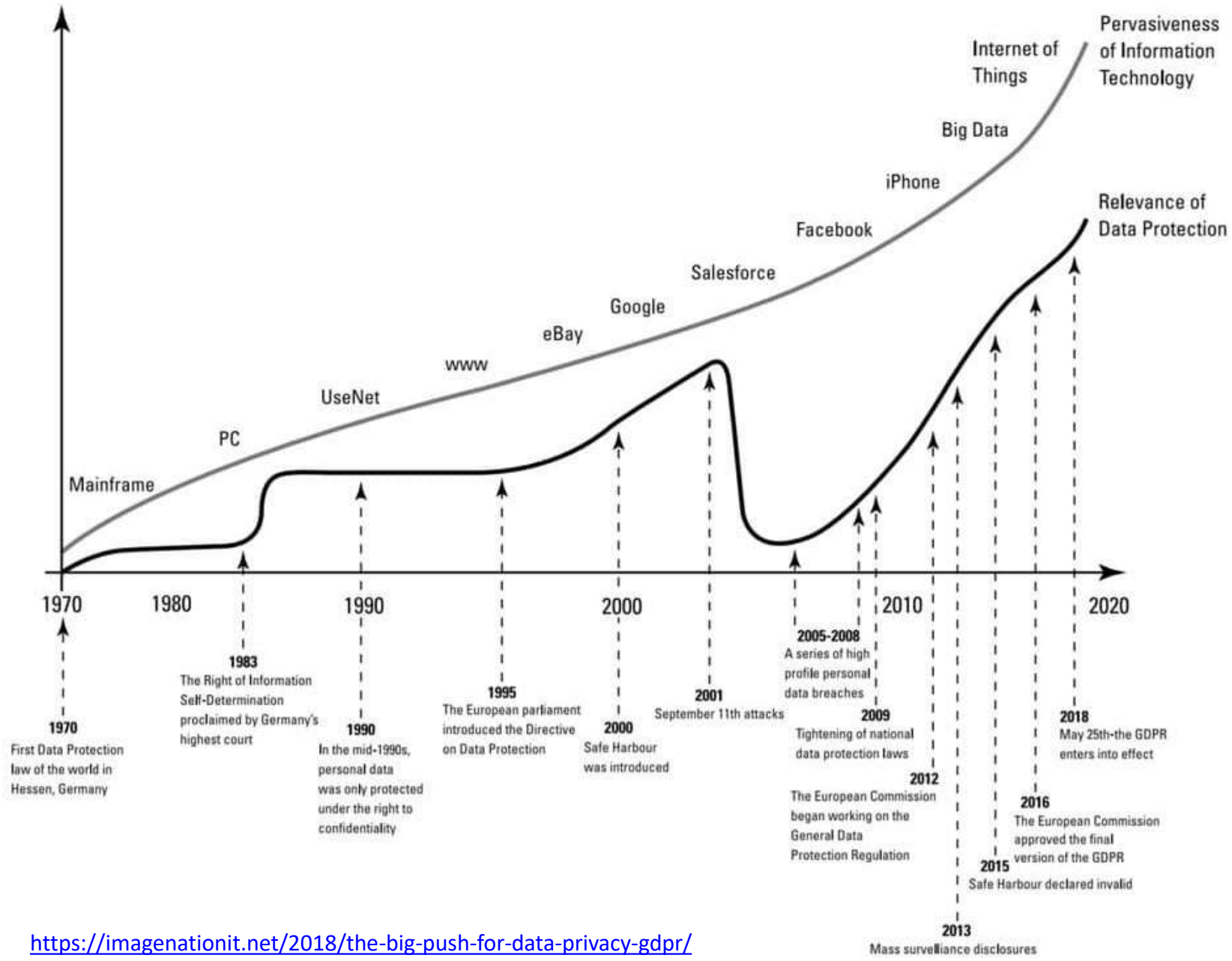
Reflection in Germany of Gestapo's privacy abuses in WW2 and Stasi's privacy abuses in East Germany



Revelations about global surveillance & existence of NSA and GCHQ

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

6 GDPR timeline



https://imagenationit.net/2018/the-big-push-for-data-privacy-gdpr/

7 Что такое GDPR?



REGULATIONS

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)

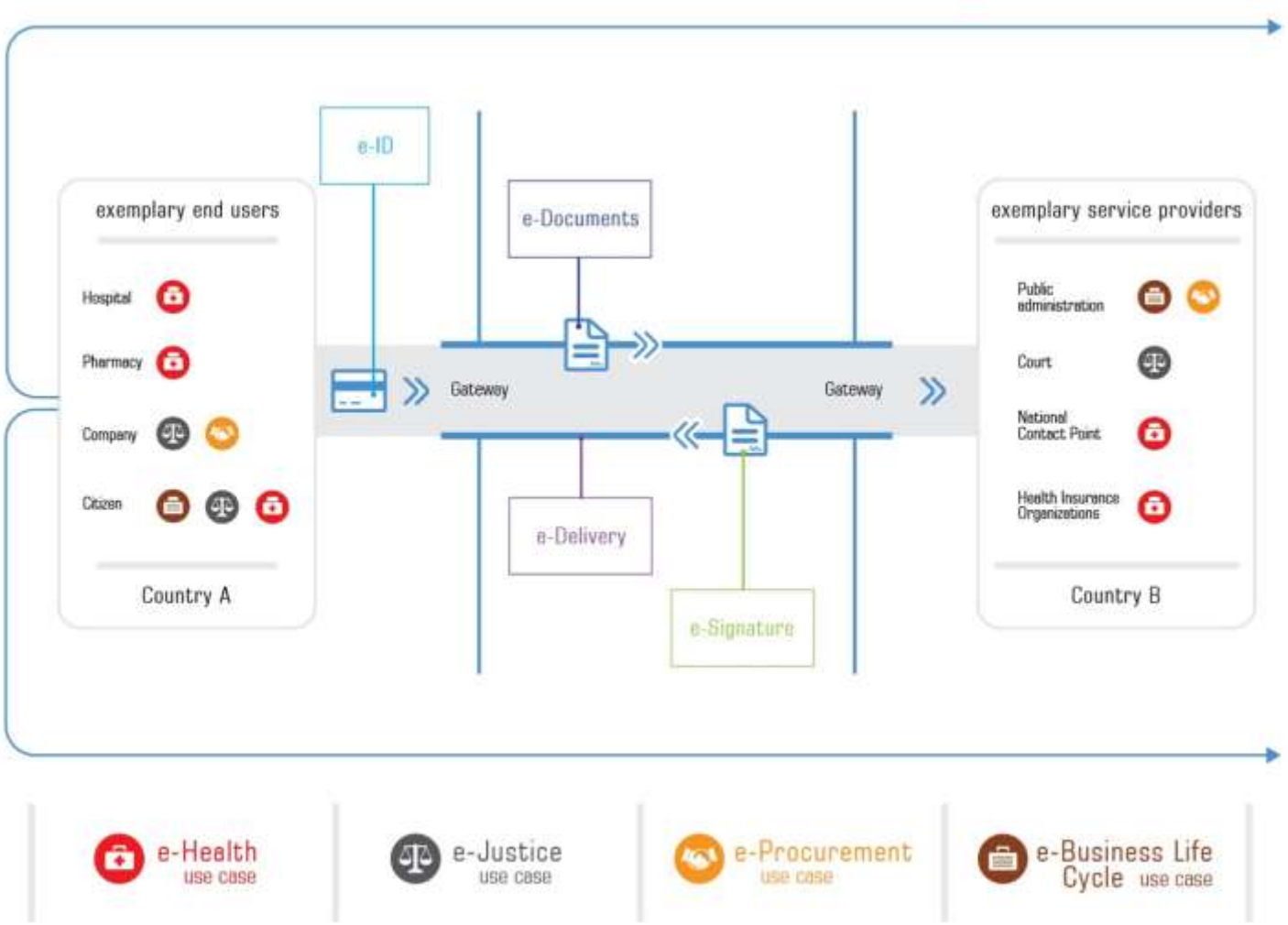
[Regulation (EU) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**) – это новый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

8 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 онлайновых бизнес-проектов, доступность контента пользователям, защищенность интересов авторов.



https://www.esens.eu/

9 GDPR как часть реформы европейского права

Обратите внимание на следующие акты, которые прямо или косвенно связаны с GDPR:

- 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**) 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) 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

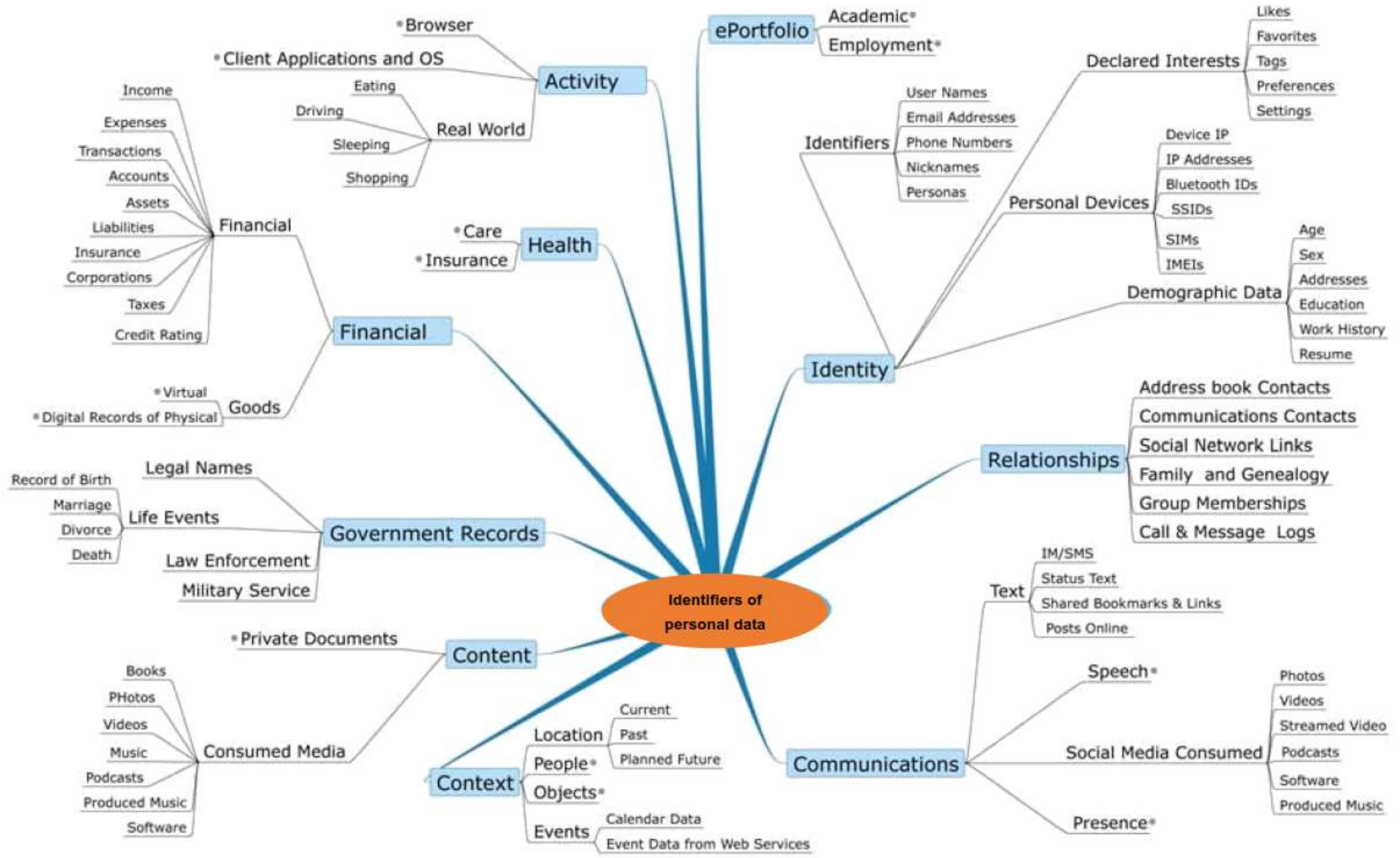
Полезные ссылки:

- 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/ЕАСТ.

10 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)

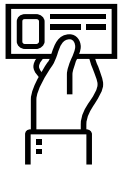
11 Персональные данные в GDPR



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

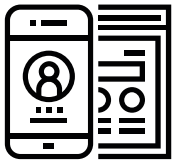
12 Источники персональных данных

Мониторинг



Предоставленные данные

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



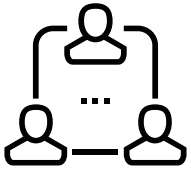
Распространенные данные

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



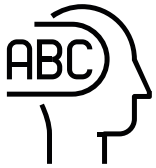
Наблюдаемые данные

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



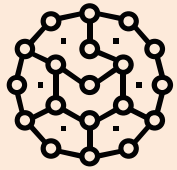
Назначенные данные

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 анализа корреляции между наборами данных, например, расчет кредитного рейтинга или прогнозирование состояния здоровья

Профилирование

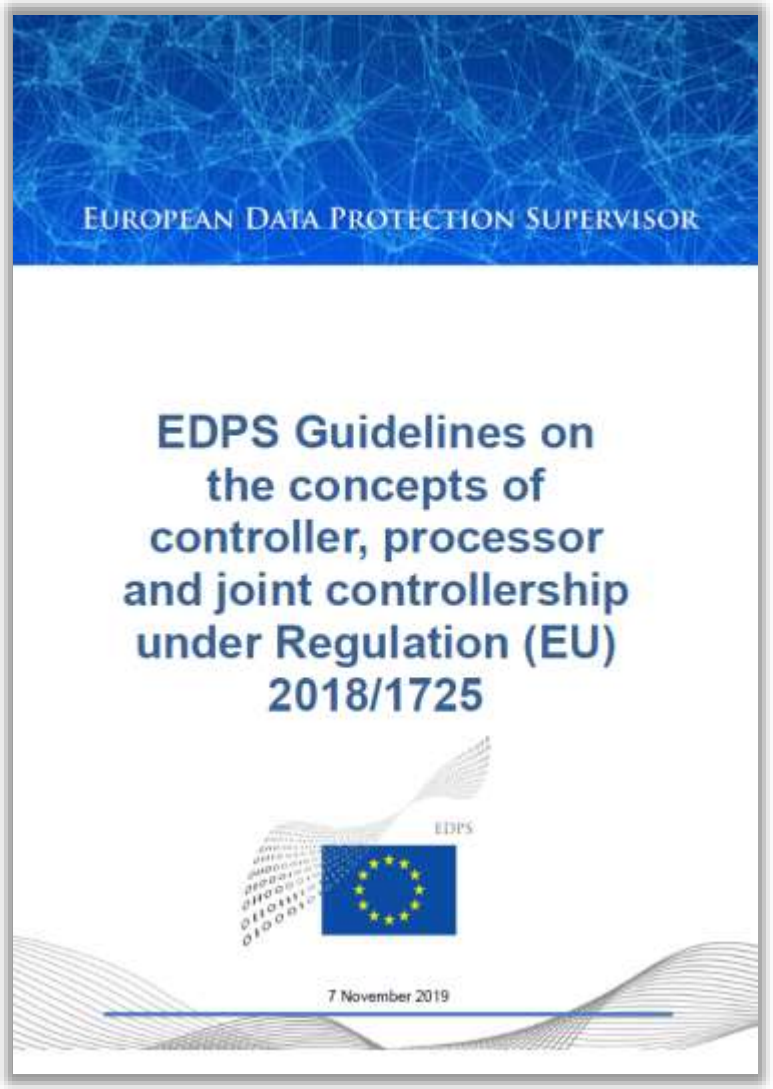
См. Abrams, Martin. The origins of personal data and its implications for governance. OECD, March 2014.

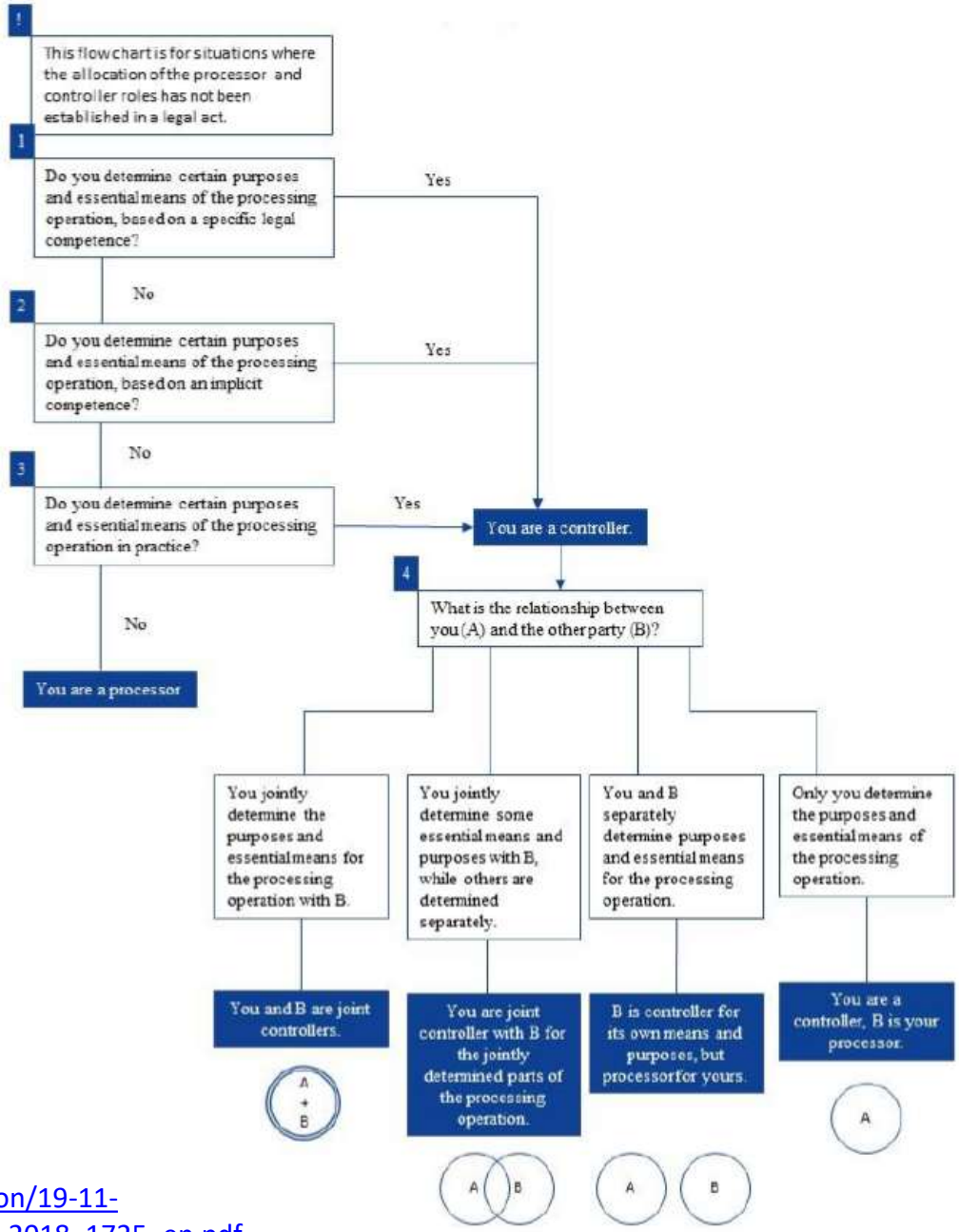
13 Принципы GDPR, изложенные простыми словами



https://dpo-net.ro/gdpr-principles-translated-into-simple-language/

Руководство EDPS по определению ролей controller, processor и and joint controlles





https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf

15 GDPR на одной странице от TeachPrivacy

TERRITORIAL SCOPE



EU Establishments

Non-EU Established Organizations

Offer goods or services or engaging in monitoring within the EU.

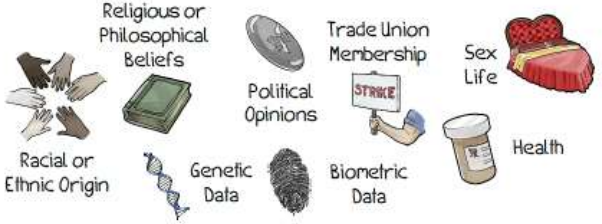
THE PLAYERS



PERSONAL DATA



SENSITIVE DATA



RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS



Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.



Record of Data Processing Activities

Maintain a documented register of all activities involving processing of EU personal data.



Data Impact Assessment

For high risk situations

Data Protection by Design

built in starting at the beginning of the design process



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.

GDPR

DATA BREACH NOTIFICATION

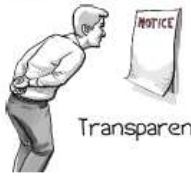


A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

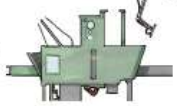
If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency



Automated Decision Making

"Right not to be subject to a decision based solely on automated processing, including profiling."



Right to Erasure



Access and Rectification



Purpose Specification and Minimization



Right to Data Portability

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



Adequate Level of Data Protection

Binding Corporate Rules (BCRs)





Privacy Shield



Model Contractual Clauses

TEACHPRIVACY www.teachprivacy.com

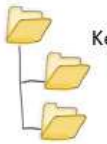
Workforce awareness training by Prof. Daniel J. Solove

Please ask permission to reuse or distribute

https://a5h8v9a3.stackpathcdn.com/wp-content/uploads/GDPR-Whiteboard-TeachPrivacy-Privacy-Awareness-Training-4.pdf

16 Высокоуровневый обзор GDPR

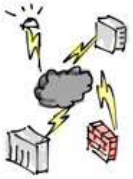
What organizations have to do



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



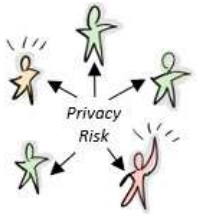
Get a parent's consent to collect data for children under 16



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



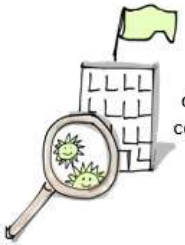
Implement Data Protection-by-Design *(Privacy "baked-in")*



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

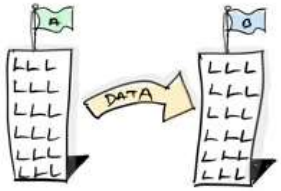
What individuals can do



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



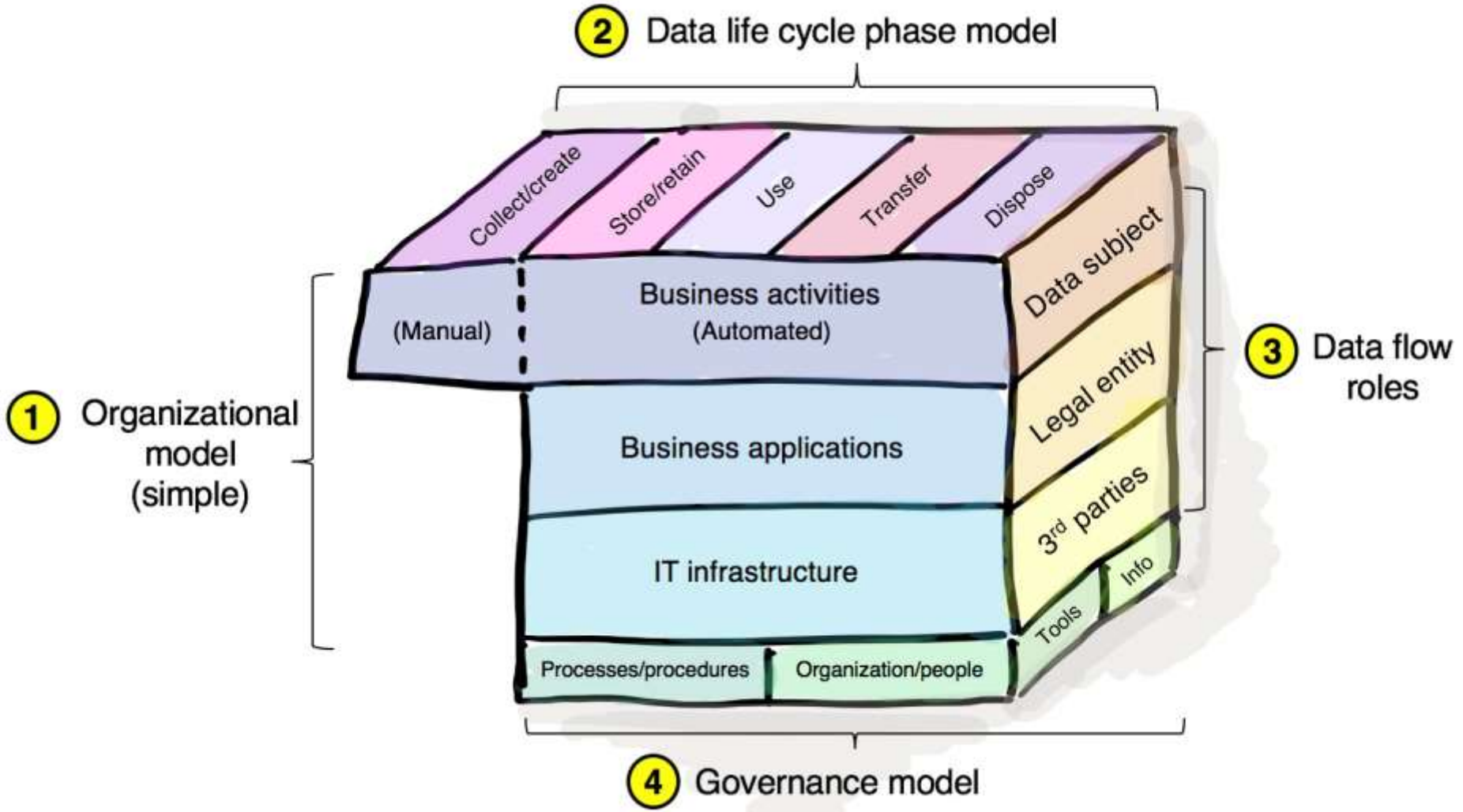
Impose temporary data processing bans, require data breach notification, or order erasure of personal data



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

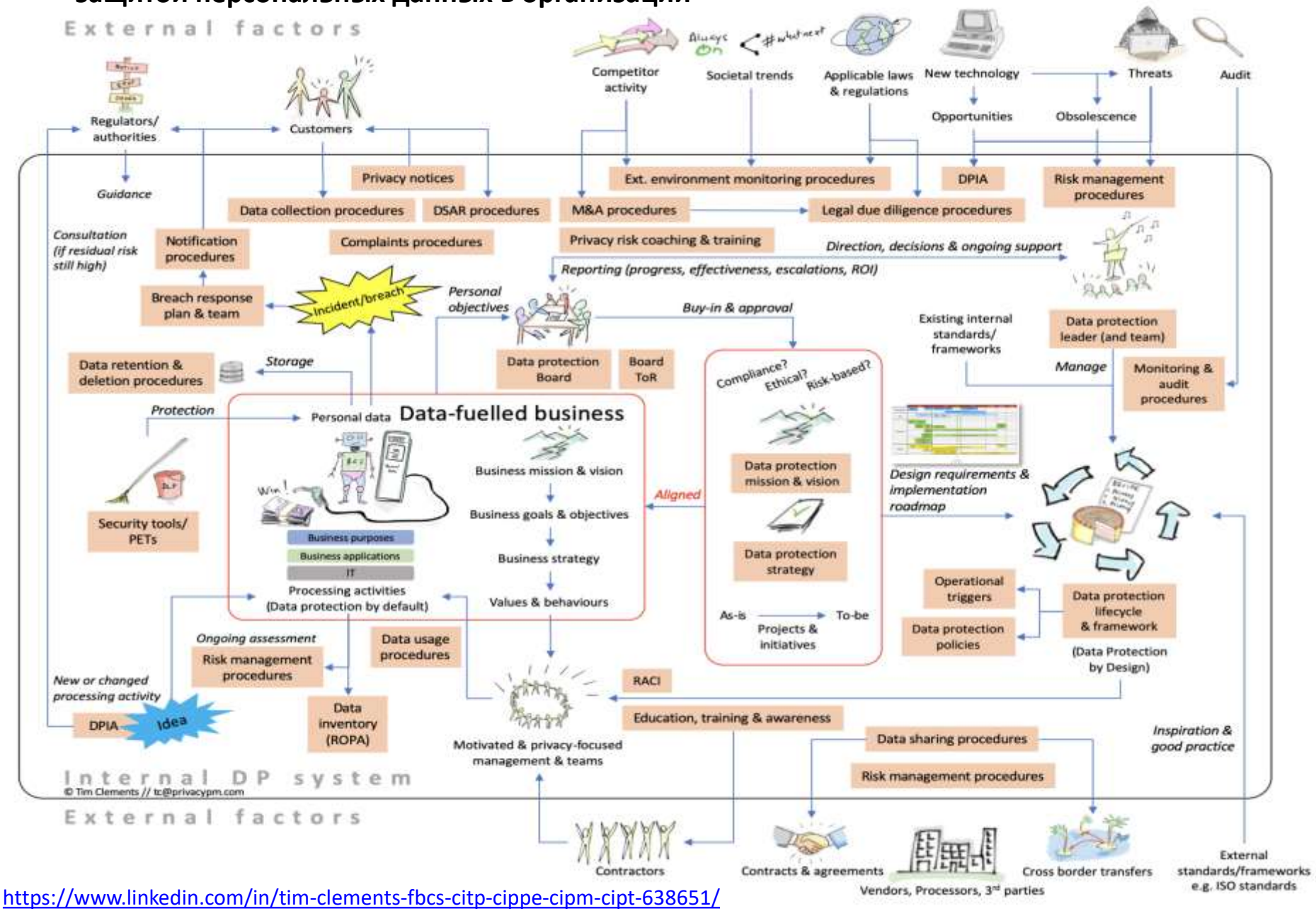
https://www.linkedin.com/in/tim-clements-fbcs-citp-cippe-cipm-cipt-638651/

Модель анализа GDPR применительно к деятельности организации



https://www.linkedin.com/pulse/gdpr-useful-analysis-models-tim-clements/

Представление системы управления обработкой и защитой персональных данных в организации



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

Механизмы GDPR, на которые стоит обратить особое внимание

- Legitimate Interests Assessment (Art.6) – Оценка сбалансированности законных интересов субъекта и контролера
- Privacy Notices (Art.12-14) - Предоставляемая информация при сборе персональных данных
- Right To Be Forgotten (Art.17) - Право на удаление данных («право на забвение»)
- Right To Data Portability (Art.20) - Право на переносимость данных
- Automated individual decision-making, including profiling (Art.22) - Автоматизированное индивидуальное принятие решений, включая составление профиля
- Data Protection By Default (Art.25) - Защита данных по умолчанию
- Data Protection By Design (Art.25, 32) - Защита данных на основе продуманных действий
- Representatives of Non-EU Controllers or Processors (Art.27) - Представители контролеров или обработчиков, не учрежденных в Евросоюзе
- Personal Data Breach Notification (Art.33) - Уведомление надзорного органа об утечке персональных данных
- Personal Data Breach Communication (Art.34) - Сообщение субъекту данных об утечке персональных данных
- Data Protection Impact Assessment[1] (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

20 Фокус на права субъектов

- 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



К оглавлению

22 Сфера действия GDPR: версия Роскомнадзора (1)

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 распрост
осуществляющ
них распростра
сфере. Об этом
Александр Жар
VIII Международ
данных».

По его словам,
участницей ме
устанавливающих порядок обработки персональных данных
«Регламент, по нашему мнению, должен учитываться только
европейских граждан российскими операторами на территор
отметив, что такая позиция соответствует общепринятым меж
персональных данных. «Считаю, что к вопросу о применимост
будет вернуться только после его вступления в законную силу
правоприменения. И когда это будет зафиксировано в междун
подчеркнул А. Жаров.

Конференция «Защита персональных данных» проводится по
– уполномоченного органа по защите прав субъектов персона

Состоялось завершающее в 2017 году заседание Консультативного совета при Уполномоченном органе по защите прав субъектов персональных данных

20 декабря 2017 года https://rkn.gov.ru/news/rsoc/news53394.htm



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

Соответствующие решения приняты Советом на последнем заседании в 2017 году, состоявшемся в Роскомнадзоре.

В ходе заседания члены Консультативного совета обсудили новые требования Европейского союза, закрепленные Общим регламентом по защите данных (General Data Protection Regulation, GDPR), устанавливающим порядок обработки персональных данных. В ноябре на VIII Международной конференции «Защита персональных данных» руководитель Роскомнадзора Александр Жаров отметил, что требования Регламента Европейского союза по защите персональных данных не будут распространяться на российских операторов, осуществляющих деятельности на территории России, поскольку Российская Федерация не является участницей международных договоров с ЕС. На них распространяется действие только российских законов в этой сфере в соответствии с общепринятыми международными принципами обработки персональных данных.

В рамках подведения итогов года на заседании было отмечено участие Консультативного совета в подготовке Методических рекомендаций по разработке отраслевого кодекса поведения в области защиты прав субъектов персональных данных, а также рекомендаций по составлению документа, определяющего политику оператора в отношении обработки персональных данных.

23 Сфера действия GDPR: версия Роскомнадзора (2)

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

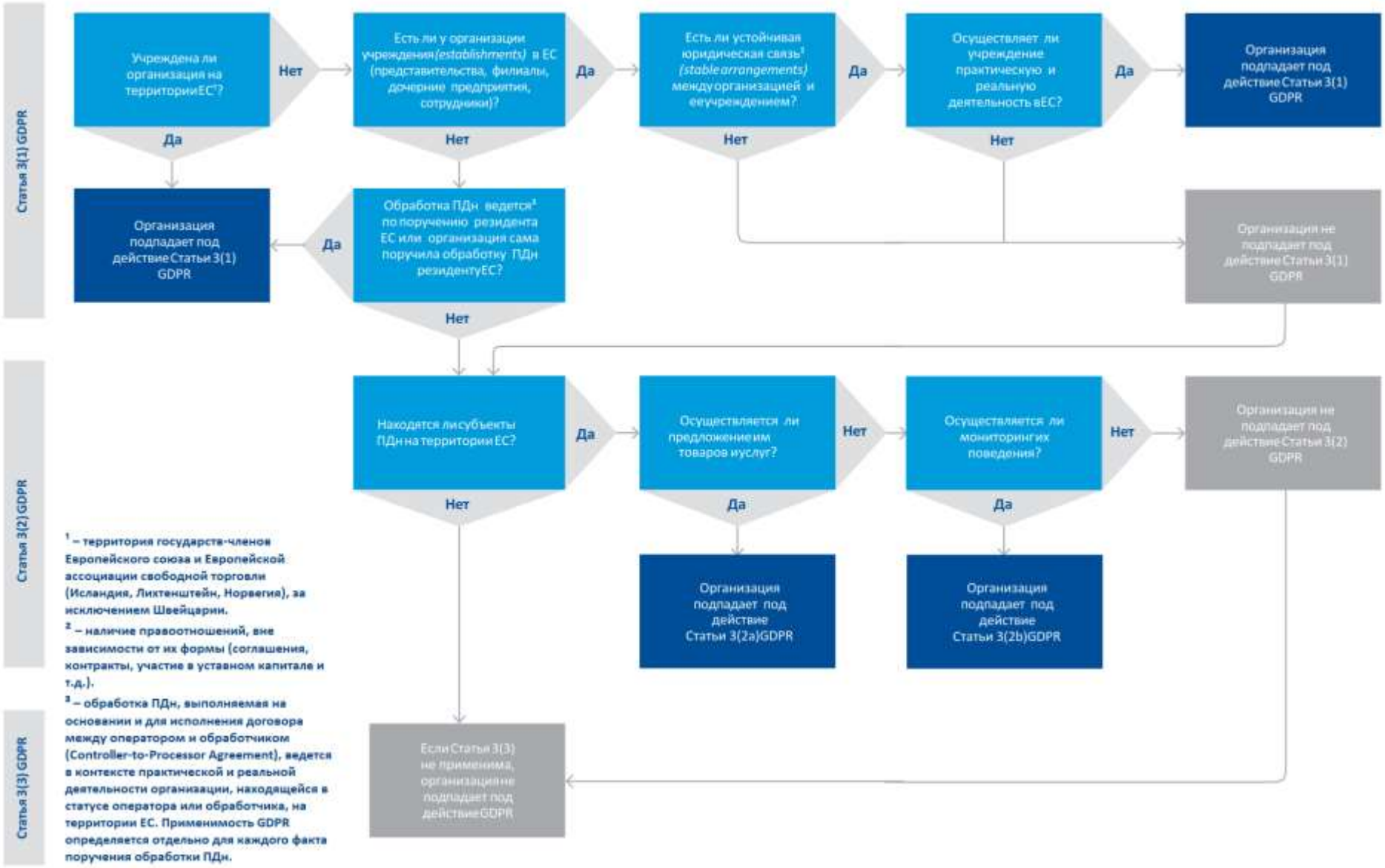
- Есть ли у компании представительства (филиалы) на территории Европейского Союза?
- Обрабатываете ли вы персональные данные граждан стран-участниц Европейского Союза по поручению европейского оператора?
- Руководствуетесь ли при осуществлении деятельности по обработке персональных данных законодательством 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.

https://rkn.gov.ru/docs/GDPR_Pankov.pdf

24 Сфера действия GDPR

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

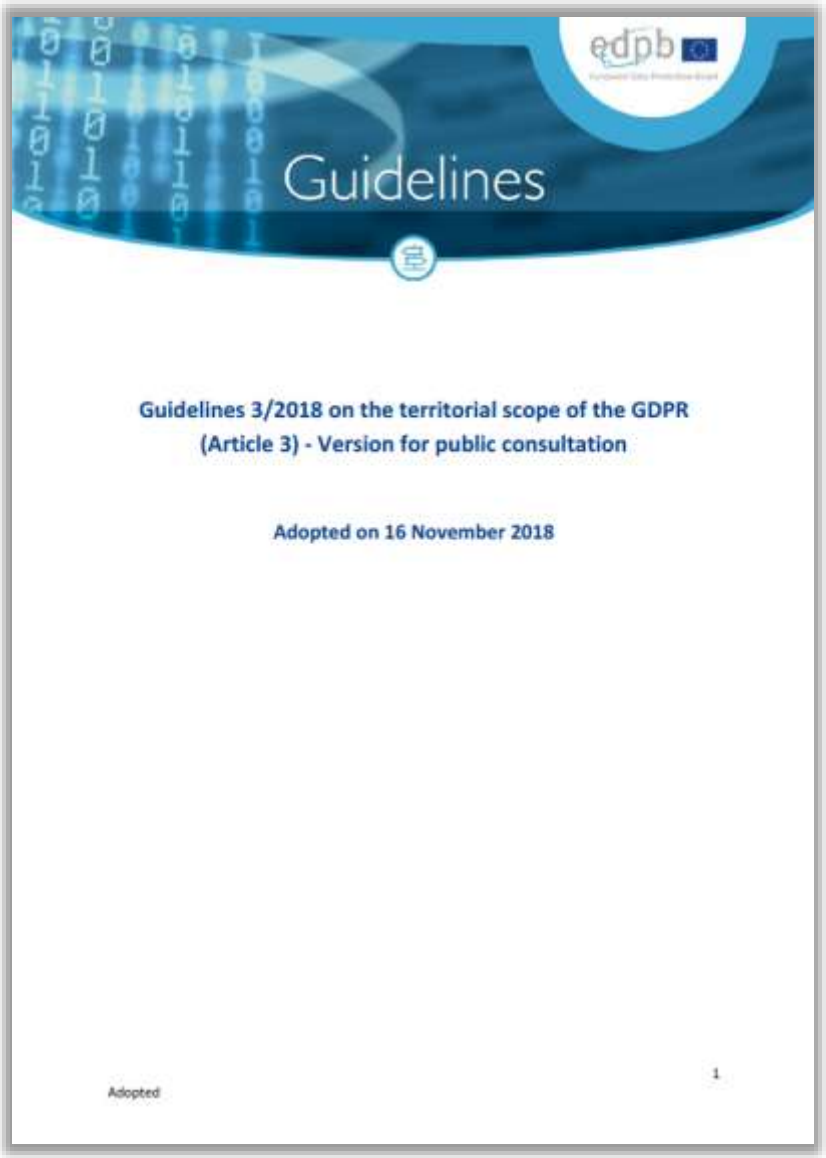


[1] – территория государств-членов Европейского союза и Европейской ассоциации свободной торговли (Исландия, Лихтенштейн, Норвегия), за исключением Швейцарии.

[2] – наличие правоотношений, вне зависимости от их формы (соглашения, контракты, участие в уставном капитале и т.д.).

[3] – обработка ПДн, выполняемая на основании и для исполнения договора между оператором и обработчиком (Controller-to-Processor Agreement), ведется в контексте практической и реальной деятельности организации, находящейся в статусе оператора или обработчика, на территории ЕС. Применимость GDPR определяется отдельно для каждого факта поручения обработки ПДн.

25 Сфера действия GDPR: разъяснения EDPB



Европейский совет по защите данных (European Data Protection Board) на своем четвертом пленарном заседании 16.11.2018 принял проект разъяснений по определению территориального охвата GDPR, которые были опубликованы 23.11.2018 для проведения общественных консультаций. 12.11.2019 была опубликована итоговая версия разъяснений.

Эти разъяснения должны способствовать формированию общих подходов в толковании сферы применения требований GDPR и прояснению порядка применения требований GDPR в отношении контролеров данных или обработчиков данных, находящихся за пределами ЕС. В разъяснениях содержатся указания относительно трактовки требований о назначении представителя в ЕС.

При подготовке разъяснений использовался подготовленный Европейской комиссией «Guide to the case law of the European Court of Justice on Articles 49 et seq. TFEU».

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf

26 Трансграничная передача персональных данных



Некоторые из целей трансграничной передачи внутри транснациональной группы

- заключение и (или) исполнение договоров и соглашений
- ведение деловых переговоров
- проявление должной осмотрительности
- участие в процедурах закупок
- осуществление информационного взаимодействия
- использование прав, исполнение обязанностей и соблюдение запретов, предусмотренных применимыми нормами

Передача персональных данных при условии соблюдения соответствующих гарантий – статья 46(1-2) GDPR



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

Соответствующие гарантии могут быть предоставлены без особого разрешения надзорного органа посредством:

(a) имеющего обязательную юридическую силу документа между органами государственной власти или правительственными учреждениями;

(b) юридически обязывающих корпоративных правил в соответствии со Статьей 47;

(c) стандартных условий о защите данных, принятых Европейской Комиссией в соответствии с процедурой проверки, указанной в Статье 93(2);

(d) стандартных условий о защите данных, принятых надзорным органом и утвержденных Европейской Комиссией согласно процедуре проверки, указанной в Статье 93(2);

(e) утвержденной нормы поведения согласно Статье 40 совместно с юридически обязывающими и защищенными обязательствами контролера или обрабатывающего данные лица в третьей стране по применению соответствующих гарантий, в том числе в отношении прав субъектов данных; или

(f) утвержденного сертификационного механизма согласно Статье 42 совместно с юридически обязывающими и защищенными обязательствами контролера или обрабатывающего данные лица в третьей стране по применению соответствующих гарантий, в том числе в отношении прав субъектов данных.

Механизмы регулирования трансграничного обмена персональных данных между резидентами РФ и ЕС/ЕАСТ

Организация в ЕС/ЕАСТ

1. Договоры гражданско-правового характера (включая Standard data protection clauses)
2. Общекорпоративные соглашения и локальные нормативные акты
3. Обязательные корпоративные правила (Binding corporate rules)
4. Специализированные соглашения, определяющие статус и роль в обработке персональных данных

Организация в РФ

Controller-to-Processor Agreement

Controller-to-Controller Agreement

! **Joint Controller** Agreement

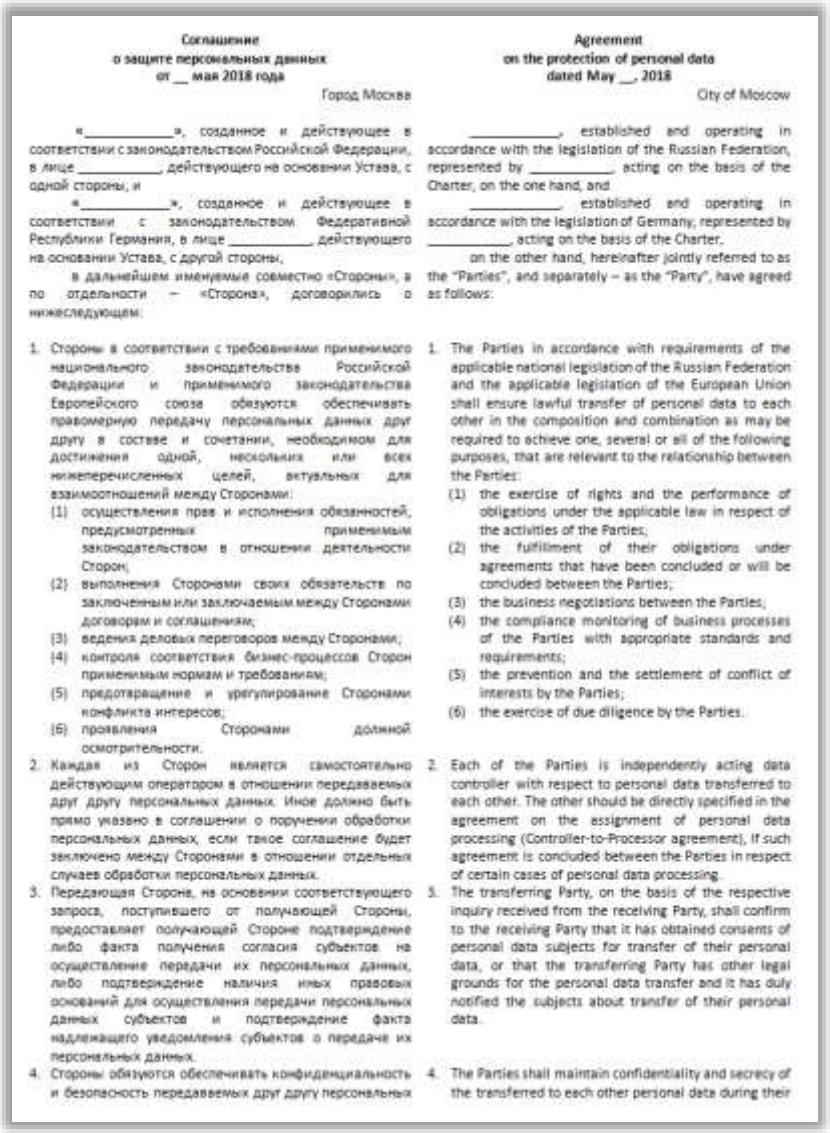
Соглашение о **поручении обработки**

Соглашение о **передаче без поручения**

*Соглашение о **совместной обработке*** ?

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

Controller-to-Controller Agreement как базовый способ построения отношений между резидентами РФ и ЕС/ЕАСТ



Соглашение
о защите персональных данных
от __ мая 2018 года

Город Москва

«_____», созданное и действующее в соответствии с законодательством Российской Федерации, в лице _____, действующего на основании Устава, с одной стороны, и

«_____», созданное и действующее в соответствии с законодательством Федеративной Республики Германия, в лице _____ действующего на основании Устава, с другой стороны,

в дальнейшем именуемые совместно «Стороны», а по отдельности – «Сторона», договорились о нижеследующем:

1. Стороны в соответствии с требованиями применимого национального законодательства Российской Федерации и применимого законодательства Европейского союза обязуются обеспечивать правомерную передачу персональных данных друг другу в составе и сочетании, необходимом для достижения одной, нескольких или всех нижеперечисленных целей, актуальных для взаимоотношений между Сторонами:
   (1) осуществления прав и исполнения обязанностей, предусмотренных применимым законодательством в отношении деятельности Сторон;
   (2) выполнения Сторонами своих обязательств по заключенным или заключаемым между Сторонами договорам и соглашениям;
   (3) ведения деловых переговоров между Сторонами;
   (4) контроля соответствия бизнес-процессов Сторон применимым нормам и требованиям;
   (5) предотвращение и урегулирование Сторонами конфликта интересов;
   (6) проявления Сторонами должной осмотрительности.
2. Каждая из Сторон является самостоятельно действующим оператором в отношении передаваемых друг другу персональных данных. Иное должно быть прямо указано в соглашении о поручении обработки персональных данных, если такое соглашение будет заключено между Сторонами в отношении отдельных случаев обработки персональных данных.
3. Передающая Сторона, на основании соответствующего запроса, поступившего от получающей Стороны, предоставляет получающей Стороне подтверждение либо факта получения согласия субъектов на осуществление передачи их персональных данных, либо подтверждение наличия иных правовых оснований для осуществления передачи персональных данных субъектов и подтверждение факта надлежащего уведомления субъектов о передаче их персональных данных.
4. Стороны обязуются обеспечивать конфиденциальность и безопасность передаваемых друг другу персональных

Agreement
on the protection of personal data
dated May __, 2018

City of Moscow

_____, established and operating in accordance with the legislation of the Russian Federation, represented by _____, acting on the basis of the Charter, on the one hand, and

_____, established and operating in accordance with the legislation of Germany, represented by _____, acting on the basis of the Charter,

on the other hand, hereinafter jointly referred to as the "Parties", and separately – as the "Party", have agreed as follows:

1. The Parties in accordance with requirements of the applicable national legislation of the Russian Federation and the applicable legislation of the European Union shall ensure lawful transfer of personal data to each other in the composition and combination as may be required to achieve one, several or all of the following purposes, that are relevant to the relationship between the Parties:
   (1) the exercise of rights and the performance of obligations under the applicable law in respect of the activities of the Parties;
   (2) the fulfillment of their obligations under agreements that have been concluded or will be concluded between the Parties;
   (3) the business negotiations between the Parties;
   (4) the compliance monitoring of business processes of the Parties with appropriate standards and requirements;
   (5) the prevention and the settlement of conflict of interests by the Parties;
   (6) the exercise of due diligence by the Parties.
2. Each of the Parties is independently acting data controller with respect to personal data transferred to each other. The other should be directly specified in the agreement on the assignment of personal data processing (Controller-to-Processor agreement), if such agreement is concluded between the Parties in respect of certain cases of personal data processing.
3. The transferring Party, on the basis of the respective inquiry received from the receiving Party, shall confirm to the receiving Party that it has obtained consents of personal data subjects for transfer of their personal data, or that the transferring Party has other legal grounds for the personal data transfer and it has duly notified the subjects about transfer of their personal data.
4. The Parties shall maintain confidentiality and secrecy of the transferred to each other personal data during their

Текст соглашения: http://sps-ib.ru/dta.docx

- ✓ определяет статус сторон как самостоятельных операторов 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.

30 GDPR и Brexit



12.11.2018 был опубликован проект Соглашения о выходе Соединенного Королевства из ЕС. Статьи 70-74 касаются вопросов защиты персональных данных, а статья 128 регламентирует вопрос участия Великобритании в Европейском совете по защите данных (European Data Protection Board).

Ключевые моменты проекта Соглашения:

- GDPR, LED, ePR и иные акты ЕС будут действовать на территории Соединенного Королевства весь переходный период (29.03.2019-01.01.2021). Аналогичный подход касается юрисдикции Суда справедливости Евросоюза (European Court of Justice);
- Великобритания с 29.03.2019 перестает участвовать в работе EDPB и в панъевропейской системе взаимодействия между надзорными органами (см. главу VII GDPR);
- до 01.01.2021 Великобритании необходимо будет урегулировать вопрос о трансграничной передаче персональных данных с ЕС согласно ст.45 GDPR (принятия ЕК решения о достаточности мер) или путем заключения отдельного соглашения с ЕС.

Кроме того, 13.12.2018 Департамент цифровых технологий, культуры, СМИ и спорта Соединенного Королевства (Department for Digital, Culture, Media and Sport) опубликовал описание правовых последствий для регулирования вопросов защиты персональных данных в случае реализации сценария «no Brexit deal».

https://ec.europa.eu/commission/files/draft-agreement-withdrawal-united-kingdom-great-britain-and-northern-ireland-european-union-and-european-atomic-energy-community-agreed-negotiators-level-14-november-2018_en

Заявление ICO о влиянии Brexit на обмен данными между ЕС/ЕАСТ и Великобританией



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.

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/statement-on-data-protection-and-brexit-implementation-what-you-need-to-do

Рекомендации, руководства и практические пособия



К оглавлению

33 Руководства, рекомендации, лучшие практики от EDPB

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

1. Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)
2. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default - version for public consultation
3. Guidelines 3/2019 on processing of personal data through video devices
4. 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)
5. 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
6. EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation
7. 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
8. EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)
9. EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
10. 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. EDPB Response to the MEP Sophie in't Veld's letter on unfair algorithms

34 Руководства, рекомендации, лучшие практики от WP29

Рекомендации Рабочей группы по защите физических лиц при обработке персональных данных (Data Protection Working Party, WP29), которая действовала до 25.05.2018. Некоторые из указанных рекомендаций продолжают действовать после расформирования Рабочей группы WP29 и передачи полномочий Европейскому совету по защите данных:

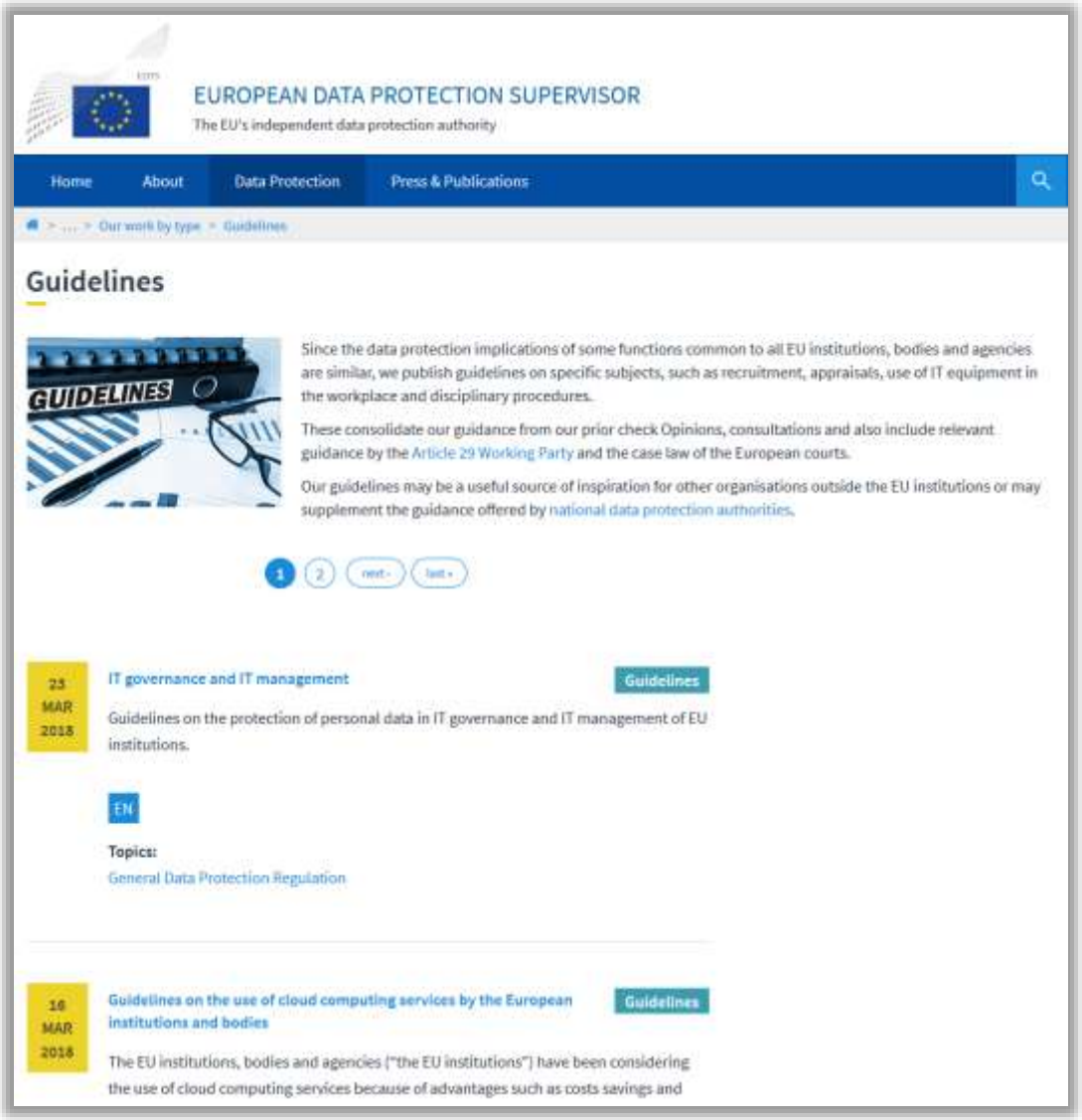
1. Guidelines on consent under Regulation 2016/679, WP259 rev.01
2. Guidelines on transparency under Regulation 2016/679, WP260 rev.01
3. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01
4. Guidelines on Personal data breach notification 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

35 Мнения, отчеты, заявления и документы от WP29

Мнения, отчеты, заявления и документы Рабочей группы по защите физических лиц при обработке персональных данных (Data Protection Working Party, WP29), которая действовала до 25.05.2018:

1. Opinion on Commission proposals on establishing a framework for interoperability - wp266
2. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) - wp247
3. Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) - wp258
4. Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) - wp252
5. Opinion 2/2017 on data processing at work - wp249
6. Opinion 03/2016 on the evaluation and review of the ePrivacy Directive wp240
7. Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain - wp179 update
8. Cookie sweep combined analysis, Report - wp229
9. Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes - wp230
10. Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones - wp231
11. Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing - wp232
12. Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes - wp234
13. Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - wp233
14. Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) - wp237
15. Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR) - wp236
16. Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision - wp238
17. Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector - wp239
18. Opinion 04/2016 on European Commission amendments proposals related to the powers of Data Protection Authorities in Standard Contractual Clauses and adequacy decisions - wp241

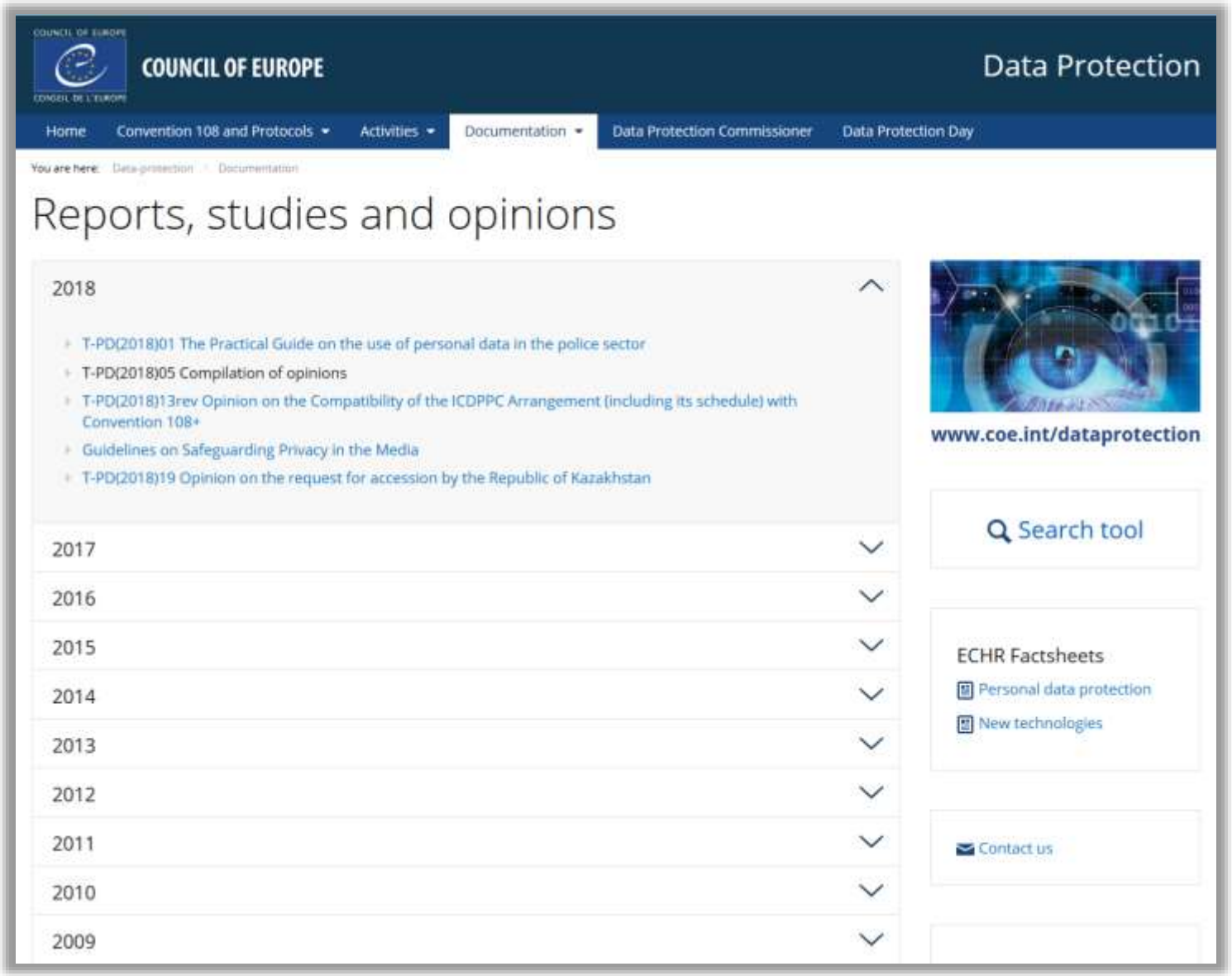
Рекомендации от Европейского инспектора по защите данных



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.

https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

База отчетов, исследований и мнений от Совета Европы по защите персональных данных



https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

38 Руководство по законодательству о защите данных от FRA

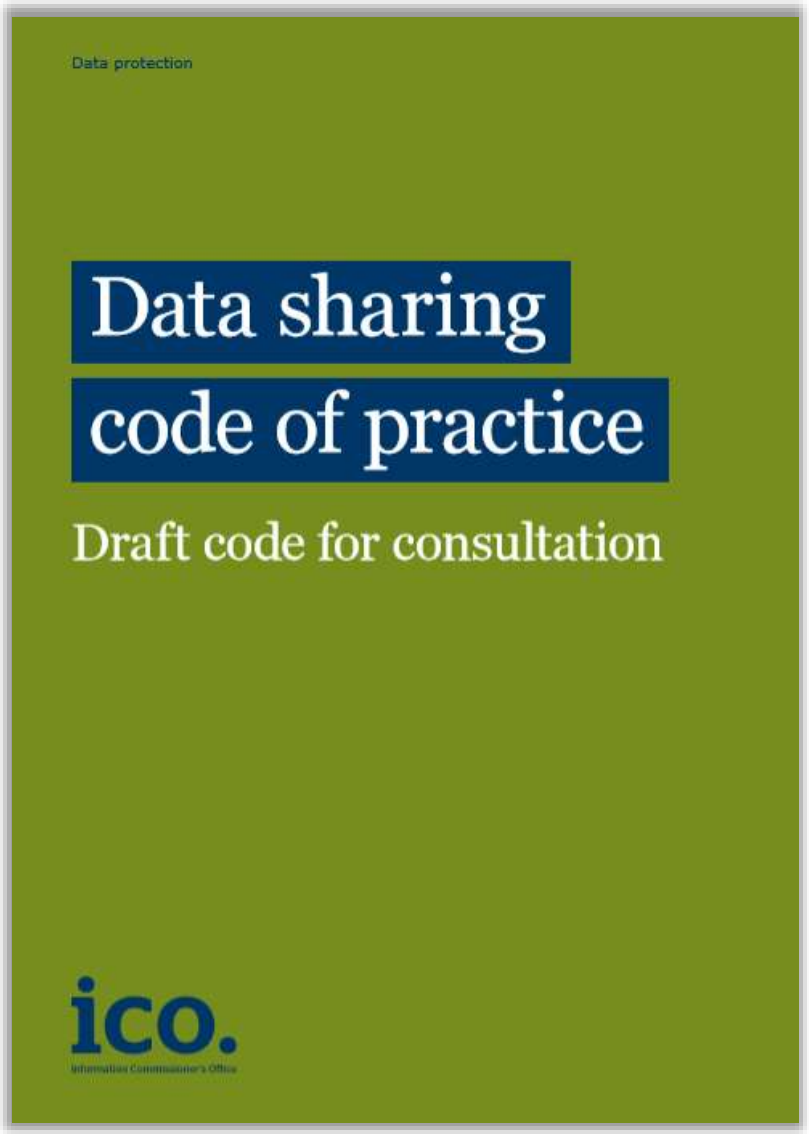


В мае 2018 года Агентство Европейского союза по фундаментальным правам человека (European Union Agency for Fundamental Rights) и Совет Европы (Council of Europe) опубликовали обновленное **Руководство по европейскому законодательству о защите данных**. Положения Руководства охватывают не только основные определения, принципы и требования GDPR, но и рассматривают применимую судебную практику Европейского суда по правам человека (European Court of Human Rights) и Европейского суда (European Court of Justice).

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

http://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

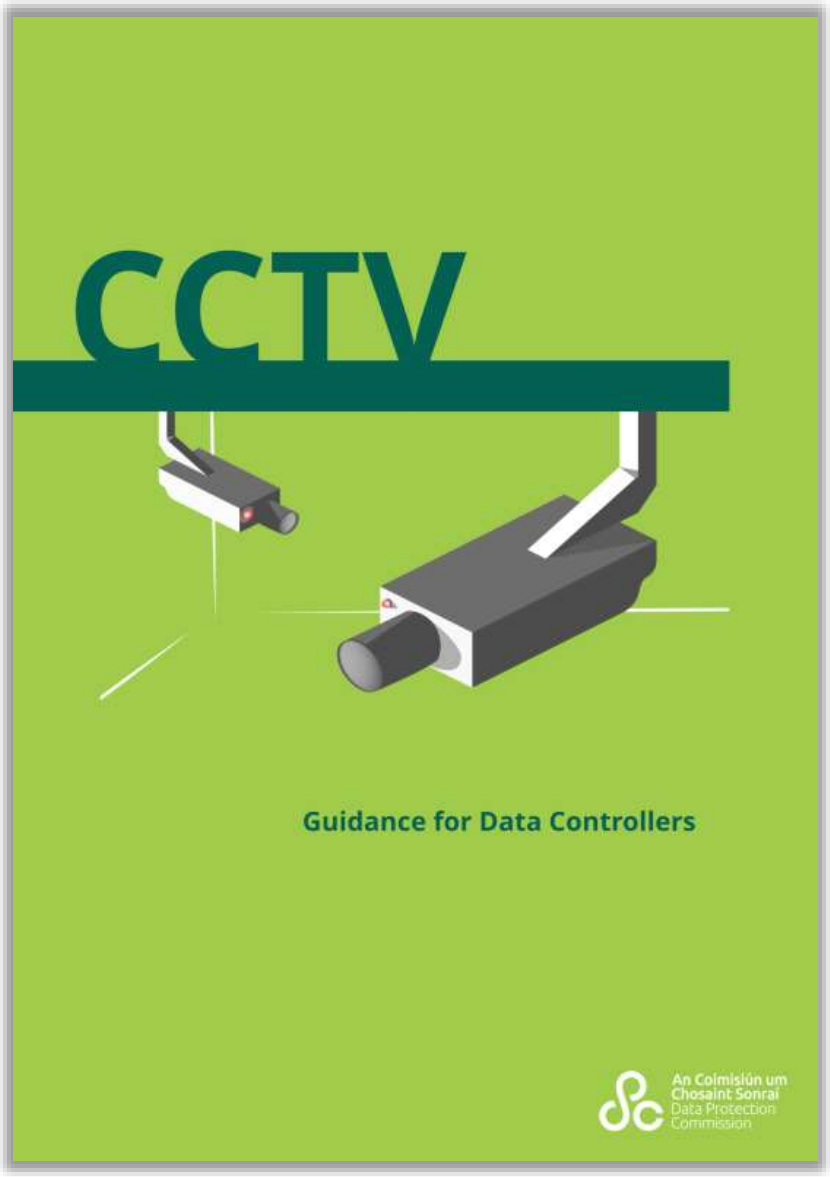
39 Кодекс поведения от ICO по предоставлению данных



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

https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

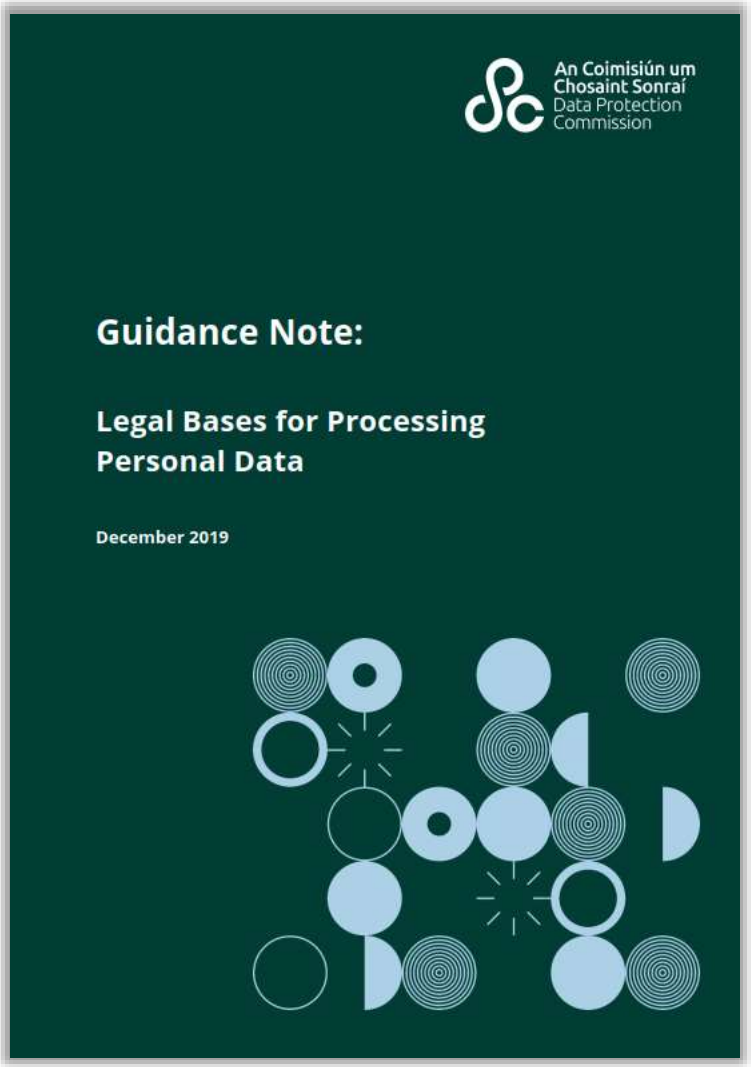
Руководство DPC по использованию систем видеонаблюдения



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

https://www.dataprotection.ie/en/guidance-landing/guidance-use-cctv-data-controllers

Руководство от DCP по определению правовой основы для обработки персональных данных



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

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

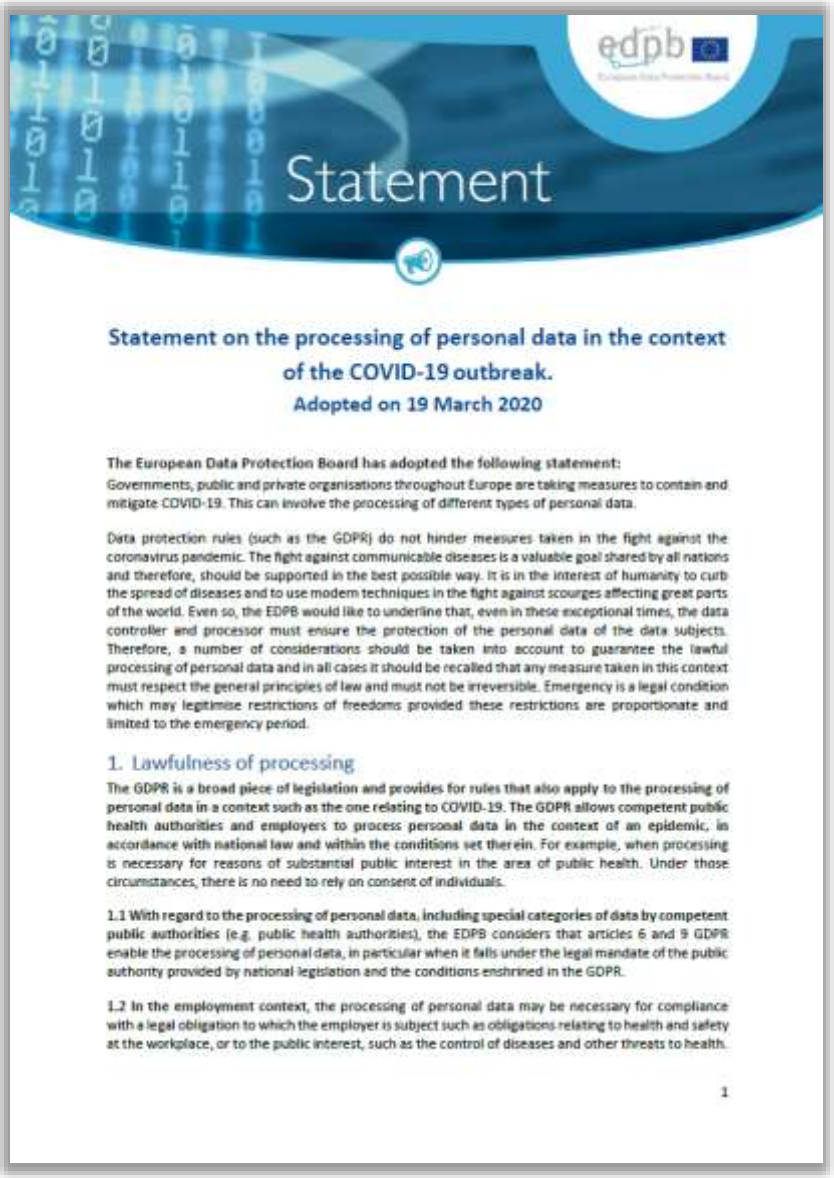
https://www.dataprotection.ie/en/guidance-landing/guidance-legal-bases-processing-personal-data

Краткое руководство от EDPS по оценке необходимости и соразмерности обработки персональных данных



https://edps.europa.eu/data-protection/our-work/publications/factsheets/edps-quick-guide-necessity-and-proportionality_en

Заявление EDPB об обработке персональных данных в контексте пандемии COVID-19



Statement

Statement on the processing of personal data in the context of the COVID-19 outbreak.
Adopted on 19 March 2020

The European Data Protection Board has adopted the following statement:
Governments, public and private organisations throughout Europe are taking measures to contain and mitigate COVID-19. This can involve the processing of different types of personal data.

Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. The fight against communicable diseases is a valuable goal shared by all nations and therefore, should be supported in the best possible way. It is in the interest of humanity to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world. Even so, the EDPB would like to underline that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data and in all cases it should be recalled that any measure taken in this context must respect the general principles of law and must not be irreversible. Emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period.

1. Lawfulness of processing

The GDPR is a broad piece of legislation and provides for rules that also apply to the processing of personal data in a context such as the one relating to COVID-19. The GDPR allows competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein. For example, when processing is necessary for reasons of substantial public interest in the area of public health. Under those circumstances, there is no need to rely on consent of individuals.

1.1 With regard to the processing of personal data, including special categories of data by competent public authorities (e.g. public health authorities), the EDPB considers that articles 6 and 9 GDPR enable the processing of personal data, in particular when it falls under the legal mandate of the public authority provided by national legislation and the conditions enshrined in the GDPR.

1.2 In the employment context, the processing of personal data may be necessary for compliance with a legal obligation to which the employer is subject such as obligations relating to health and safety at the workplace, or to the public interest, such as the control of diseases and other threats to health.

1

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.

https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en

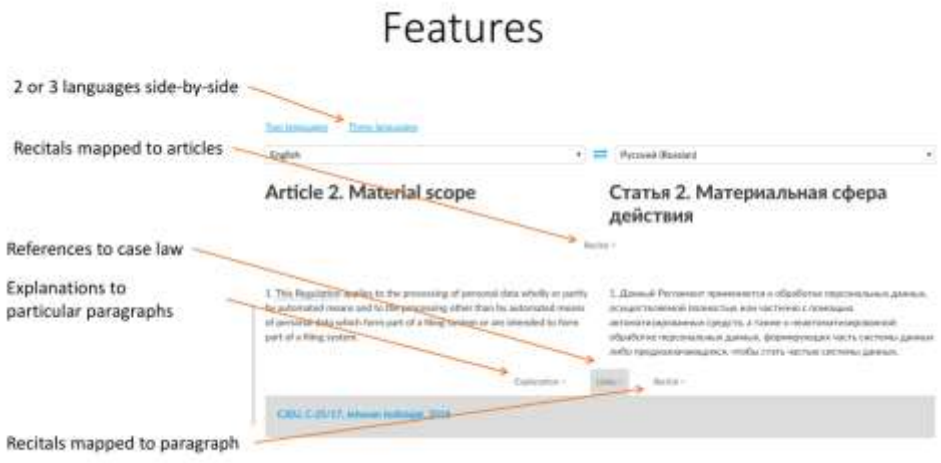
Вспомогательная информация от коммерческих и некоммерческих организаций



К оглавлению

45 GDPR на русском языке от команды Data Privacy Office





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: Например:
  - процессор вместо обработчика;
  - контролер вместо контроллера;
  - 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.

https://gdpr-text.com/

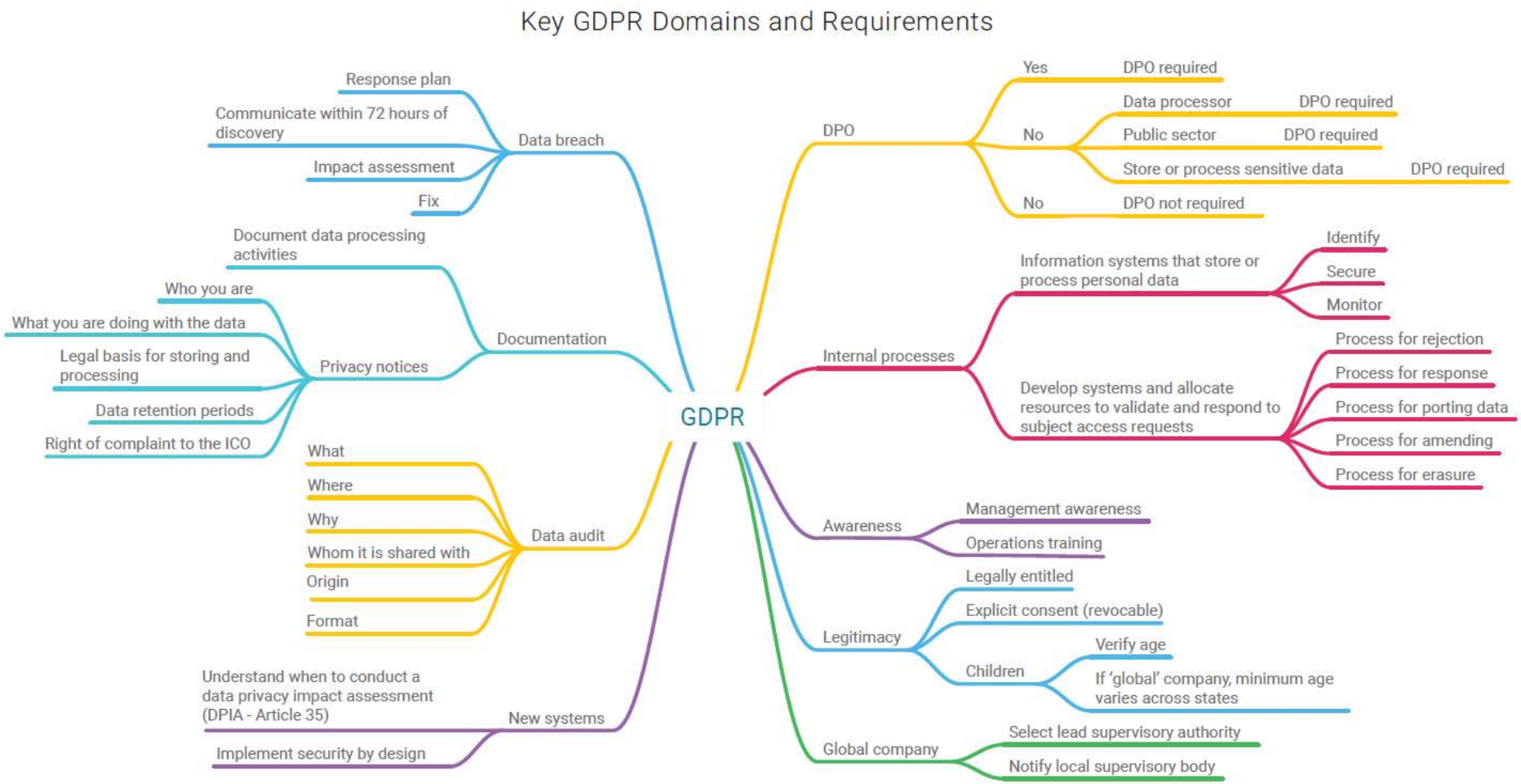
46 Соблюдение GDPR при подборе персонала



Ответы от компании SmartRecruiters на часто задаваемые вопросы об обработке персональных данных соискателей при процессе подбора персонала. Рассматриваются общие вопросы обработки персональных данных соискателей, получения их согласия, привлечение третьих лиц к обработке, сбор персональных данных соискателей из открытых источников, документирование процесса подбора персонала с точки зрения требований GDPR.

https://www.smartrecruiters.com/resources/gdpr-recruiting/recruitment-gdpr-faq/

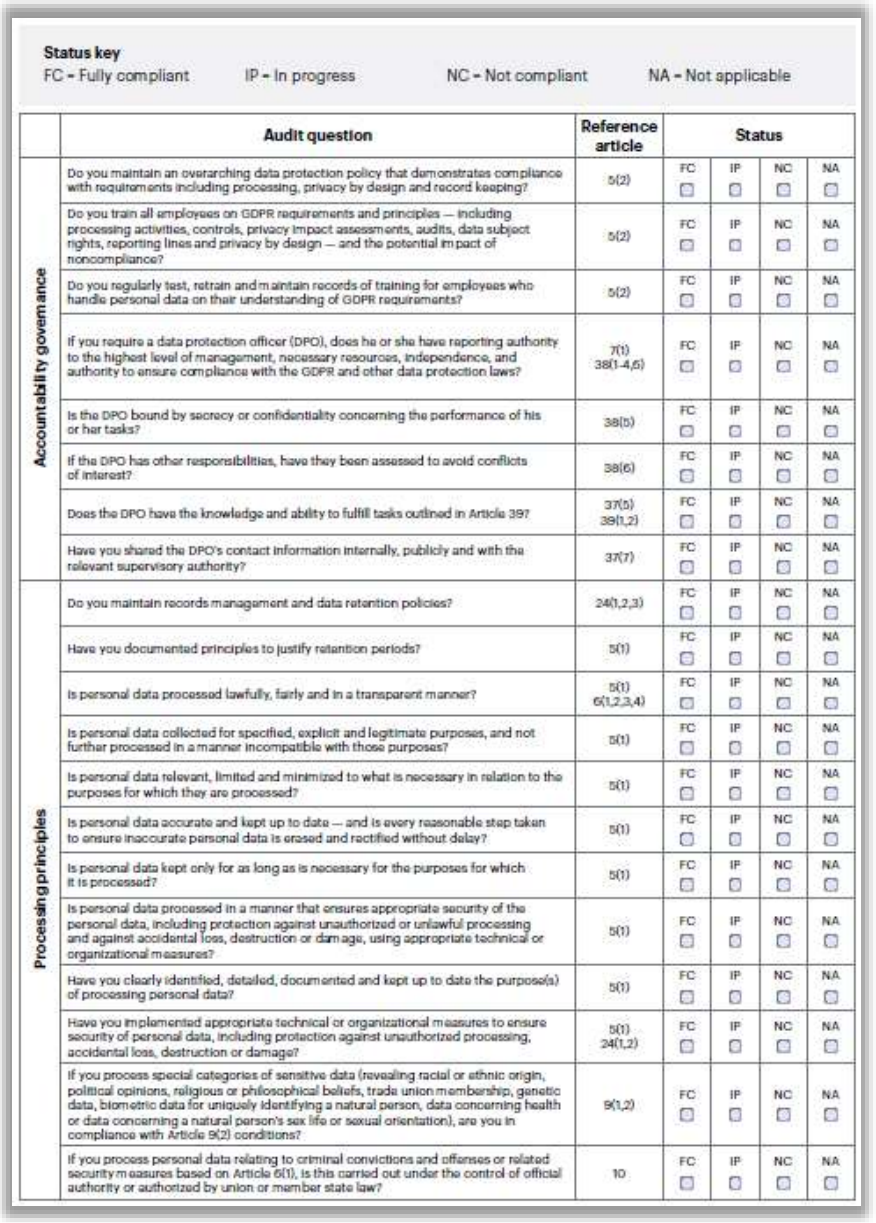
47 Пособие по аудиту выполнения требований GDPR от ISACA



https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/How-to-Audit-GDPR.aspx

48 Чеклист по аудиту выполнения требований GDPR от Gartner



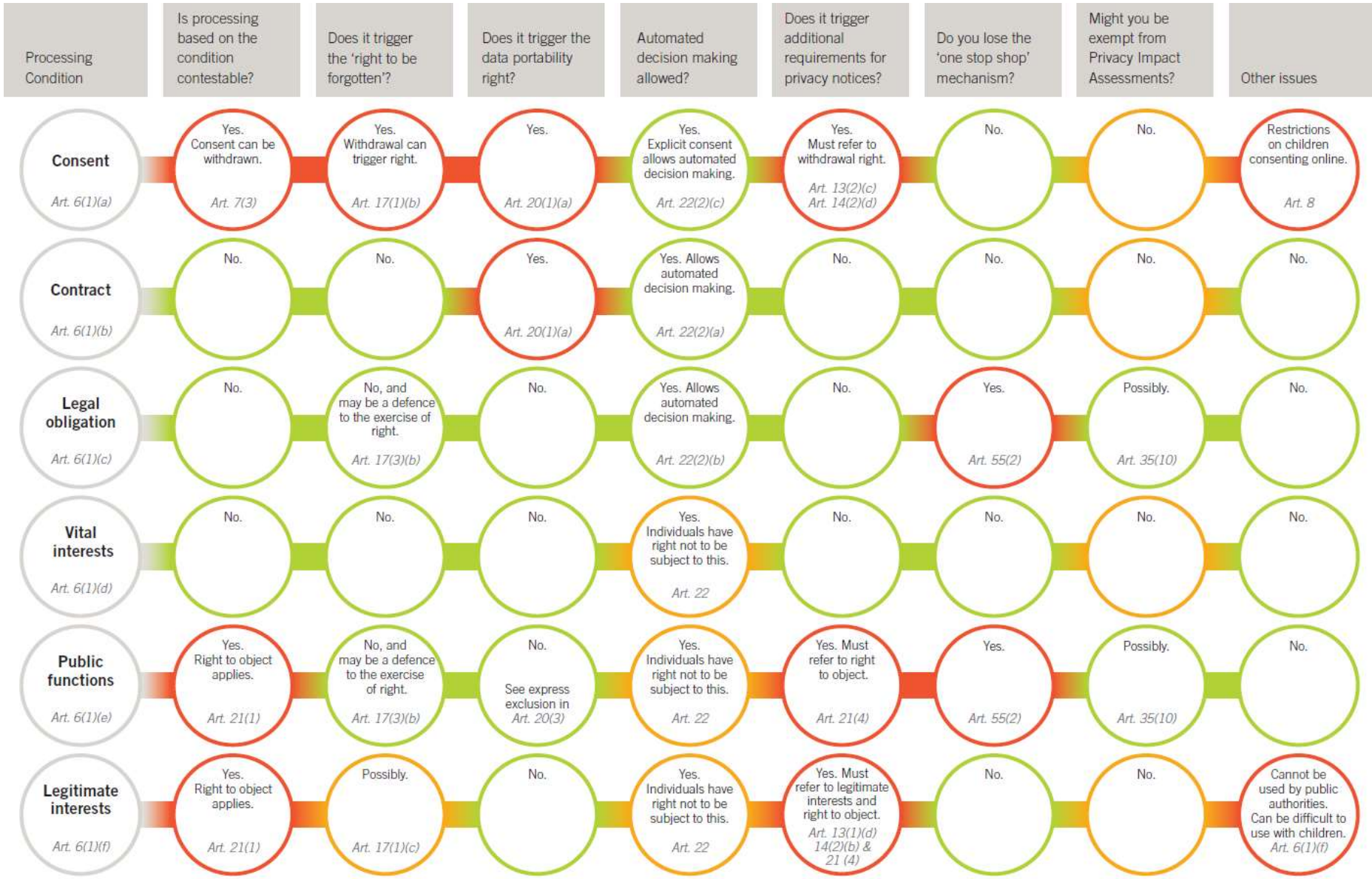


Status key
FC = Fully compliant IP = In progress NC = Not compliant NA = Not applicable

	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 ☐
	Have you shared the DPO's contact information internally, publicly and with the relevant supervisory authority?	37(7)	FC ☐	IP ☐	NC ☐	NA ☐
Processing principles	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 ☐

https://emtemp.gcom.cloud/ngw/globalassets/en/legal-compliance/documents/trends/gdpr-compliance-audit-checklist.pdf

49 «Руководство по выживанию» с GDPR от Linklaters

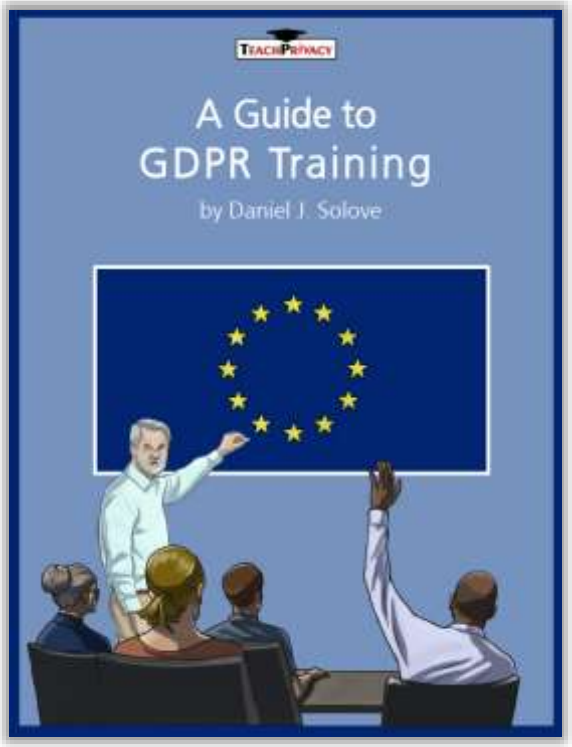


https://lpscdn.linklaters.com/-/media/files/linklaters/pdf/mkt/london/tmt_data_protection_survival_guide_singles.ashx

50 Руководства по учету требований GDPR при разработке ПО

- **Для веб-разработчиков**: руководство по приватности для браузеров от команды разработчиков Chrome
- **Для разработчиков приложений**: руководство по защите конфиденциальности пользователей, составленное Atlassian для разработчиков приложений, в котором описаны требования GDPR, а также обязанности разработчиков и некоторые практические примеры по исполнении 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

Краткое руководство TeachPrivacy по подготовке и проведению тренингов по GDPR



(1) Motivation: Why should people care?

(2) Definition: What is personal data?

(3) Responsibilities: What should people know about the way the organization handles privacy? What should people do in their jobs to protect data?



Motivation

If people don't care, they won't pay attention and won't change their behavior. People need to understand why privacy matters and the concrete implications that violations of privacy can have on individuals, on the organization, and on the workforce members involved in a violation. People pay a lot more attention when they are told why they should be paying attention.

Definition

People need to know what data is covered. People must learn roughly how to identify personal data and sensitive data. A challenge here is that the GDPR has a definition of personal data that is different from how US law defines it. US law defines it in many different ways.



People don't need to know each particular definition — otherwise, their heads would spin. The key goal here is to get people to understand that a lot of data that they might not think is personal data in fact can be personal data. Data that alone is not identified to a particular person can be combined with other data and become identified to that person. So it isn't possible to provide a comprehensive list of all personal data.

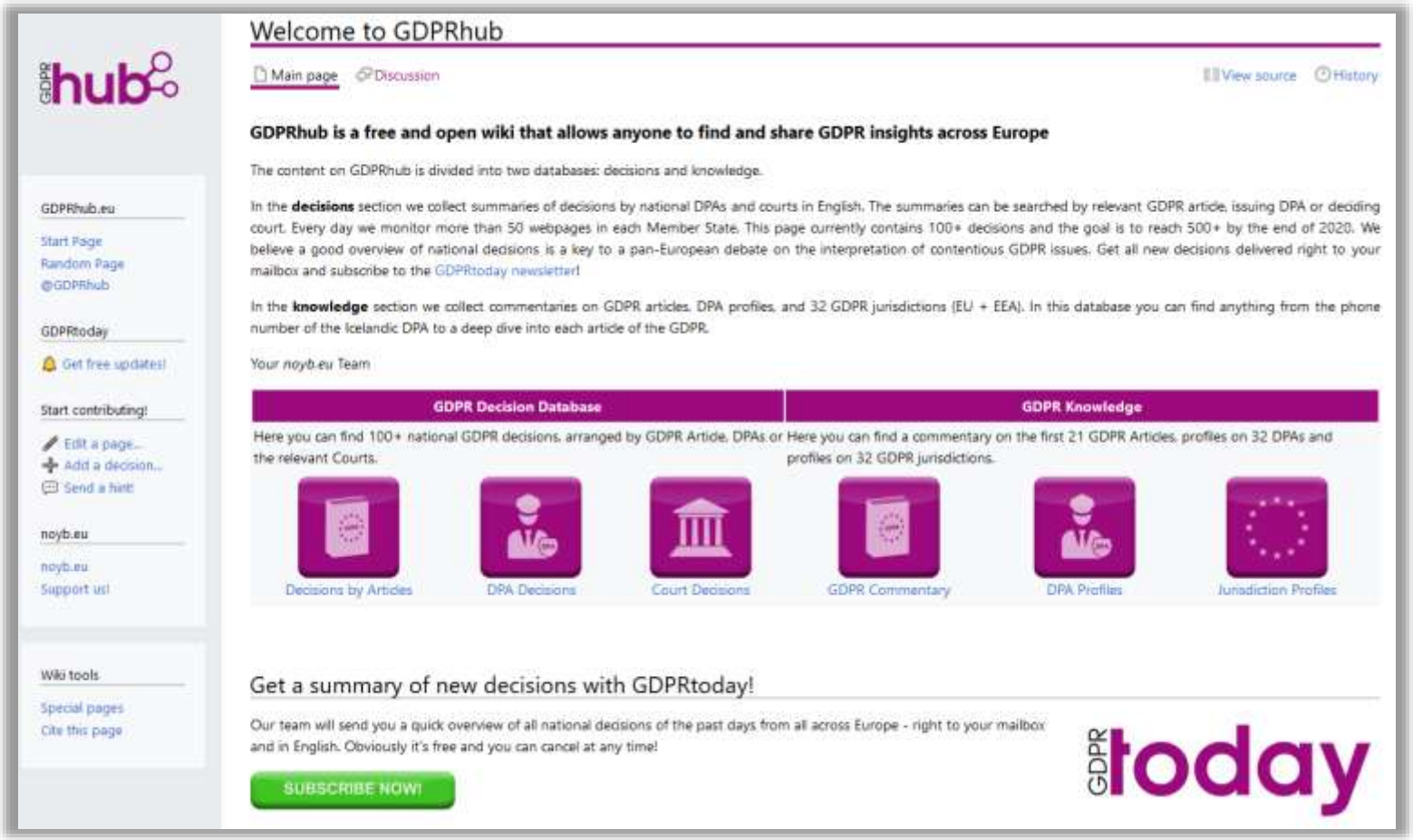
My strategy here is to deepen people's understanding and teach them enough so that they ask when they are uncertain and avoid making false assumptions.

Responsibilities

People need to be taught what they should know about how an organization handles its responsibilities for protecting data as well as their role in the process. This can be accomplished by teaching people what protecting privacy entails more conceptually. By this, I mean that training should focus on the Fair Information Practice Principles (FIPPs). The FIPPs are the backbone to most privacy laws, and despite all the differences in privacy laws around the world, the FIPPs have widespread consensus.

https://a5h8v9a3.stackpathcdn.com/wp-content/uploads/2019/04/GDPR-Training-Guide-TeachPrivacy-Privacy-Awareness-Training.pdf

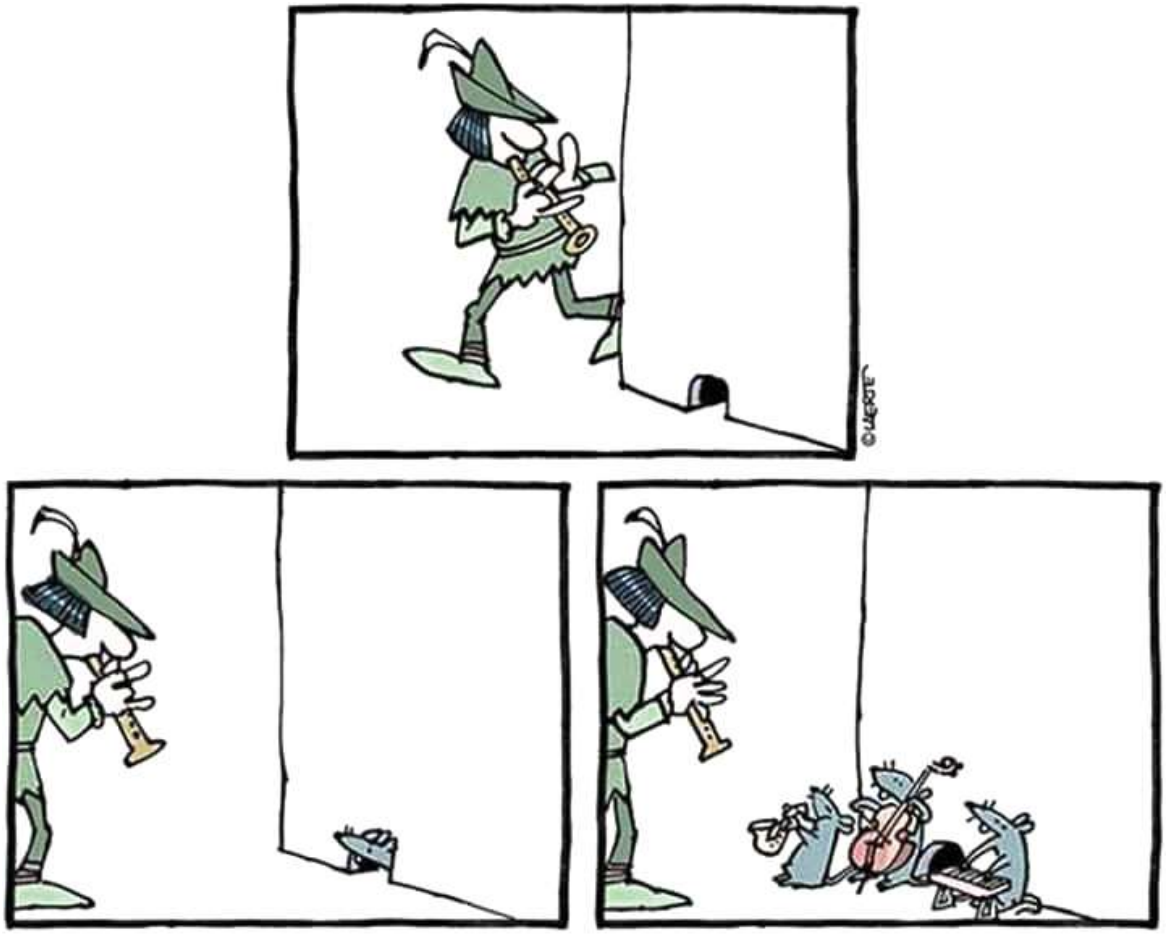
Краткое руководство TeachPrivacy по подготовке и проведению тренингов по GDPR



НКО "None of Your Business" («Не твое 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 дает 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.

https://gdprhub.eu

Data Protection Officer



К оглавлению

DPO как центральное звено в процессах комплаенса по персональным данным



Самостоятельность и независимость DPO

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 и обрабатывающее данные лицо должны гарантировать, что DPO принимает своевременное и надлежащее участие в решении всех вопросов, связанных с защитой персональных данных

Art.38(3)

Контролер и обрабатывающее данные лицо должны гарантировать, что DPO не получает иных указаний относительно выполнения указанных задач.

DPO не должен быть отстранен или оштрафован контролером или обрабатывающим данные лицом за выполнение своих задач.

Art.38(6)

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

Потенциальный конфликт интересов DPO

- DPO может являться сотрудником контролера или обрабатывающего данные лица, 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 дорожащим своей **репутацией**.



Управление риском конфликта интересов для DPO

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



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.

https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels

Руководство для DPO от T4DATA



Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

T4DATA

The DPO Handbook

Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation

By Douwe Korff and Marie Georges
drawing on major contributions by the project partners
under the Training Data Protection Authorities and Data Protection Officers - T4DATA project
(Grant Agreement number: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

Project Partners

Fondazione Lelio e Lisli Basso – ONLUS (Italy)
Coordinator

FONDAZIONE LELIO E LISLI BASSO

and

Garante per la Protezione dei Dati Personali (Italy)

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Agencia de Proteccion de Datos (Spain)

Agencija za zastitu osobnih podataka (Croatia)

Commission for Personal Data Protection (Bulgaria)

Urząd Ochrony Danych Osobowych (Poland)

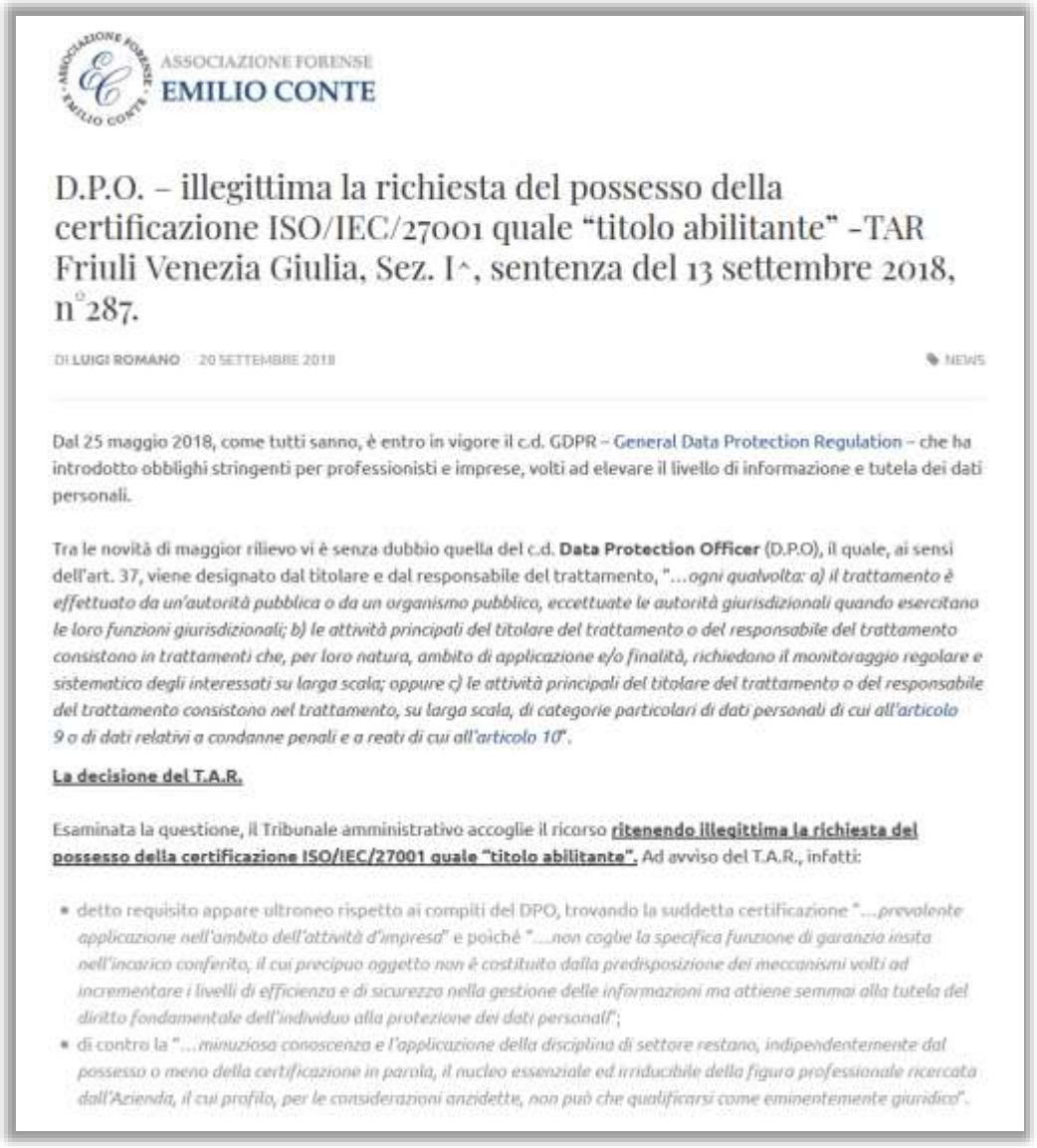
The DPO Handbook

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

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

https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf

TAR Friuli Venezia Giulia о требованиях к DPO



ASSOCIAZIONE FORENSE
EMILIO CONTE

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.

https://associazioneforenseemilioconte.it/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/

61 Независимость DPO стоит дорого



THE IRISH TIMES

Sun, Dec 9, 2018

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

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

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

Public Services Card

Éire | Ireland

Williams-Fitzpatrick

Seosaimhin Eilionor

01-01-2015 T0001324

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

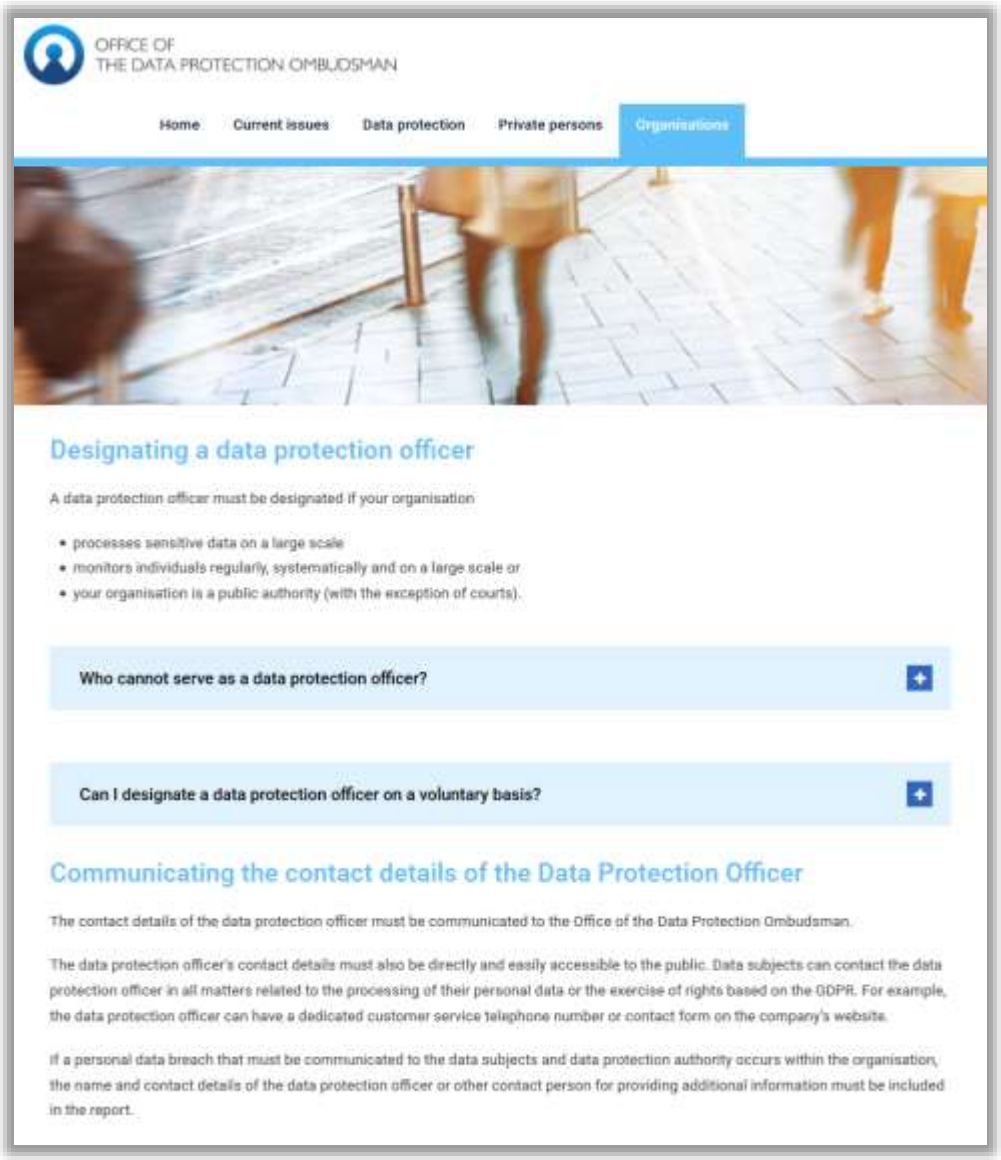
The Data Protection Commission has said it is investigating "potential breaches" of the General Data Protection Regulation by a Government department, following a complaint that it allegedly interfered with the role of its data protection officer, an offence under the EU legislation.

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-0hcqrrlh3

62 Особенности назначения DPO по мнению финского DPA



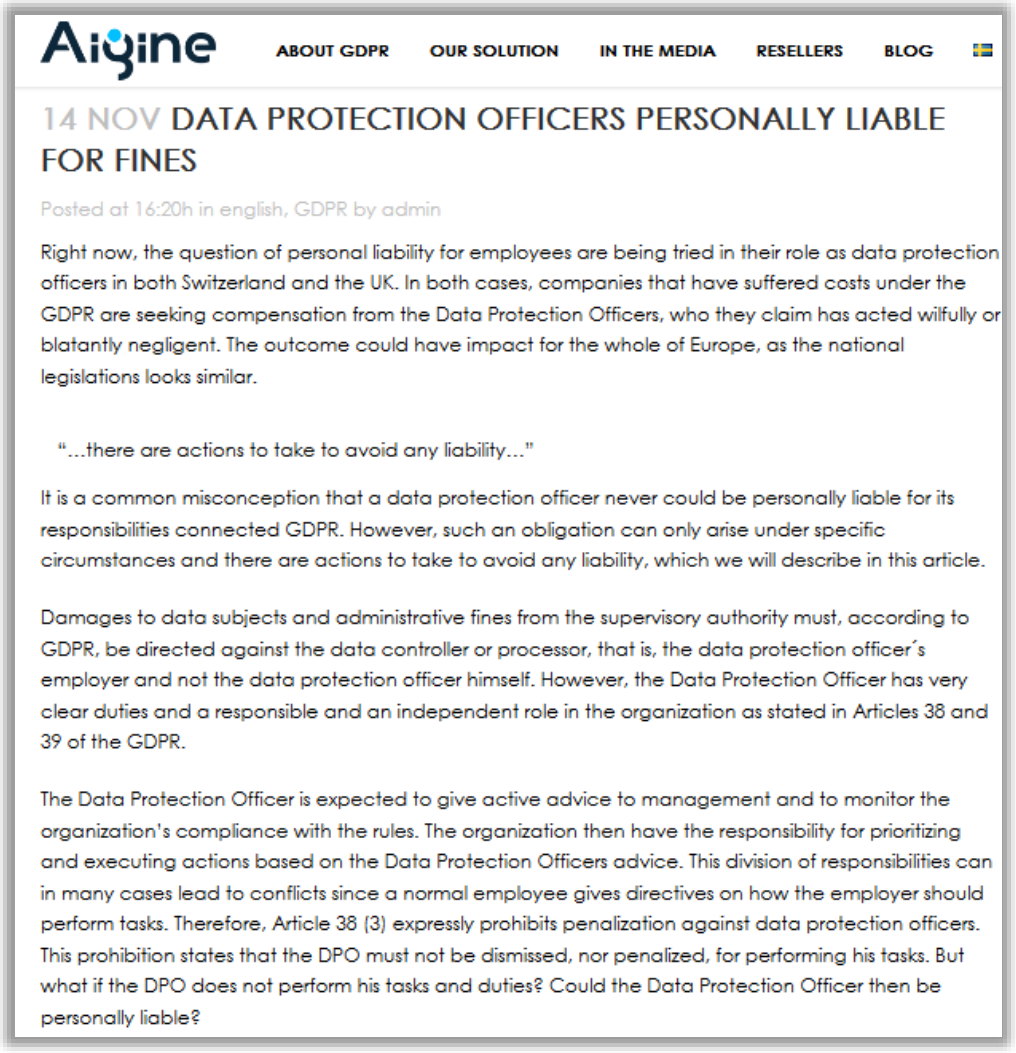
DPO не может занимать должность или осуществлять функции, которые будут требовать от него определить цели и методы обработки персональных данных. Определение целей и методов обработки персональных данных является обязанностью контролера.

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.

https://tietosuoja.fi/en/designating-a-data-protection-officer

63 Личная ответственность DPO в Европе



Aigine ABOUT GDPR OUR SOLUTION IN THE MEDIA RESELLERS BLOG

14 NOV DATA PROTECTION OFFICERS PERSONALLY LIABLE FOR FINES

Posted at 16:20h in english, GDPR by admin

Right now, the question of personal liability for employees are being tried in their role as data protection officers in both Switzerland and the UK. In both cases, companies that have suffered costs under the GDPR are seeking compensation from the Data Protection Officers, who they claim has acted wilfully or blatantly negligent. The outcome could have impact for the whole of Europe, as the national legislations looks similar.

"...there are actions to take to avoid any liability..."

It is a common misconception that a data protection officer never could be personally liable for its responsibilities connected GDPR. However, such an obligation can only arise under specific circumstances and there are actions to take to avoid any liability, which we will describe in this article.

Damages to data subjects and administrative fines from the supervisory authority must, according to GDPR, be directed against the data controller or processor, that is, the data protection officer´s employer and not the data protection officer himself. However, the Data Protection Officer has very clear duties and a responsible and an independent role in the organization as stated in Articles 38 and 39 of the GDPR.

The Data Protection Officer is expected to give active advice to management and to monitor the organization's compliance with the rules. The organization then have the responsibility for prioritizing and executing actions based on the Data Protection Officers advice. This division of responsibilities can in many cases lead to conflicts since a normal employee gives directives on how the employer should perform tasks. Therefore, Article 38 (3) expressly prohibits penalization against data protection officers. This prohibition states that the DPO must not be dismissed, nor penalized, for performing his tasks. But what if the DPO does not perform his tasks and duties? Could the Data Protection Officer then be personally liable?

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.

https://aigine.se/en/data-protection-officers-personally-liable-for-fines/gdpr/

64 Личная ответственность DPO в Южной Корее



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.

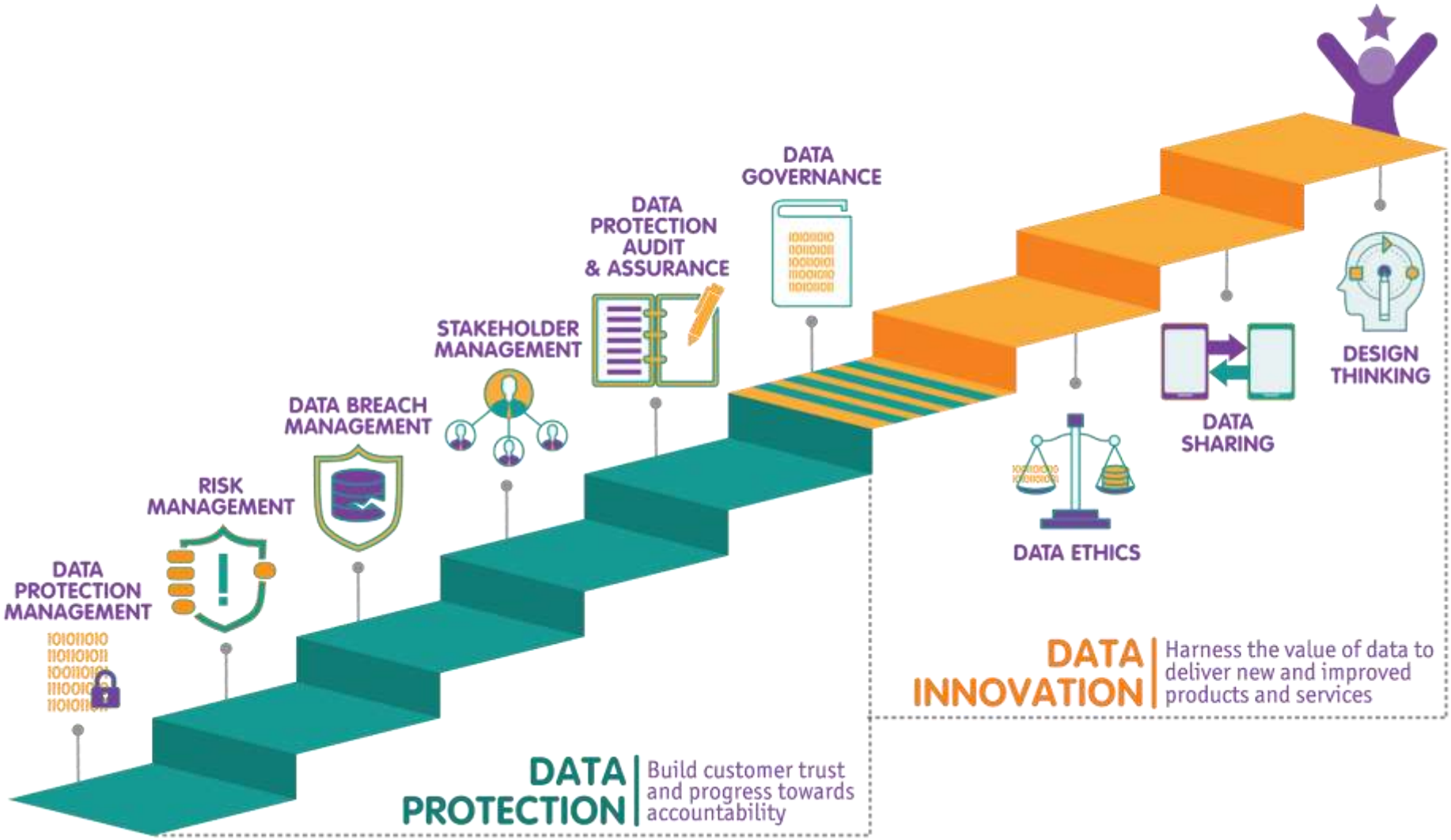
6 января 2020 года Сеульский восточный окружной суд признал Ким Джин-Хвана, DPO южнокорейского туристического агентства Hana Tour Service Inc., виновным в халатности из-за неспособности предотвратить утечку данных 2017 года, которая затронула 465,000 клиентов агентства и 29,000 сотрудников Hana Tour.

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 переснальных 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.

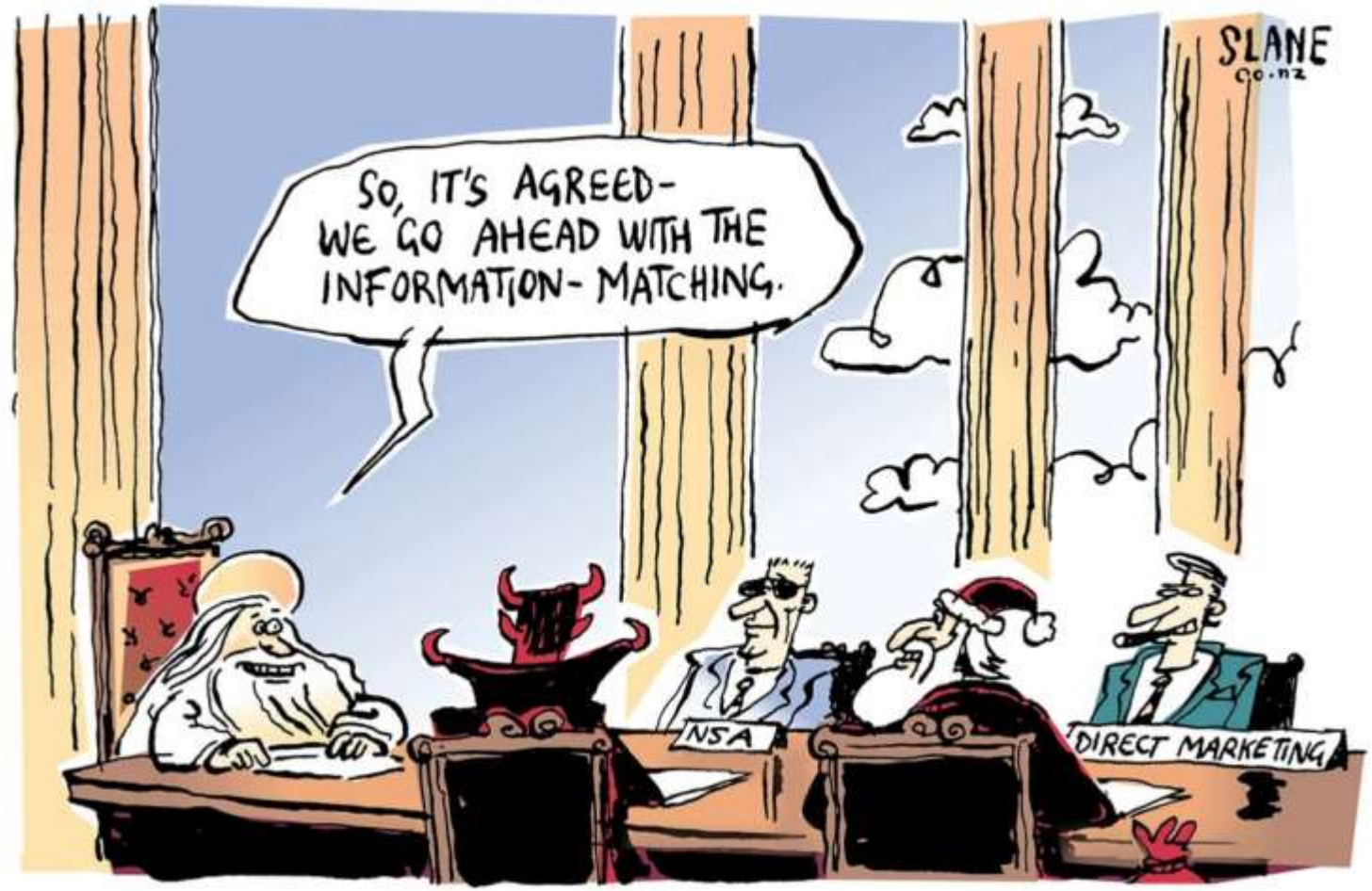
https://www.huntonprivacyblog.com/2020/01/09/south-korean-court-imposes-personal-liability-on-privacy-officer-for-data-breach/

Описание компетенций и дорожной карты развития DPO от Комиссии по защите персональных данных Сингапура



https://www.pdpc.gov.sg/dp-competency

Legitimate Interests



К оглавлению

Руководство от ICO по Legitimate Interests

Sample LIA template

ico. Information Commissioner's Office

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.

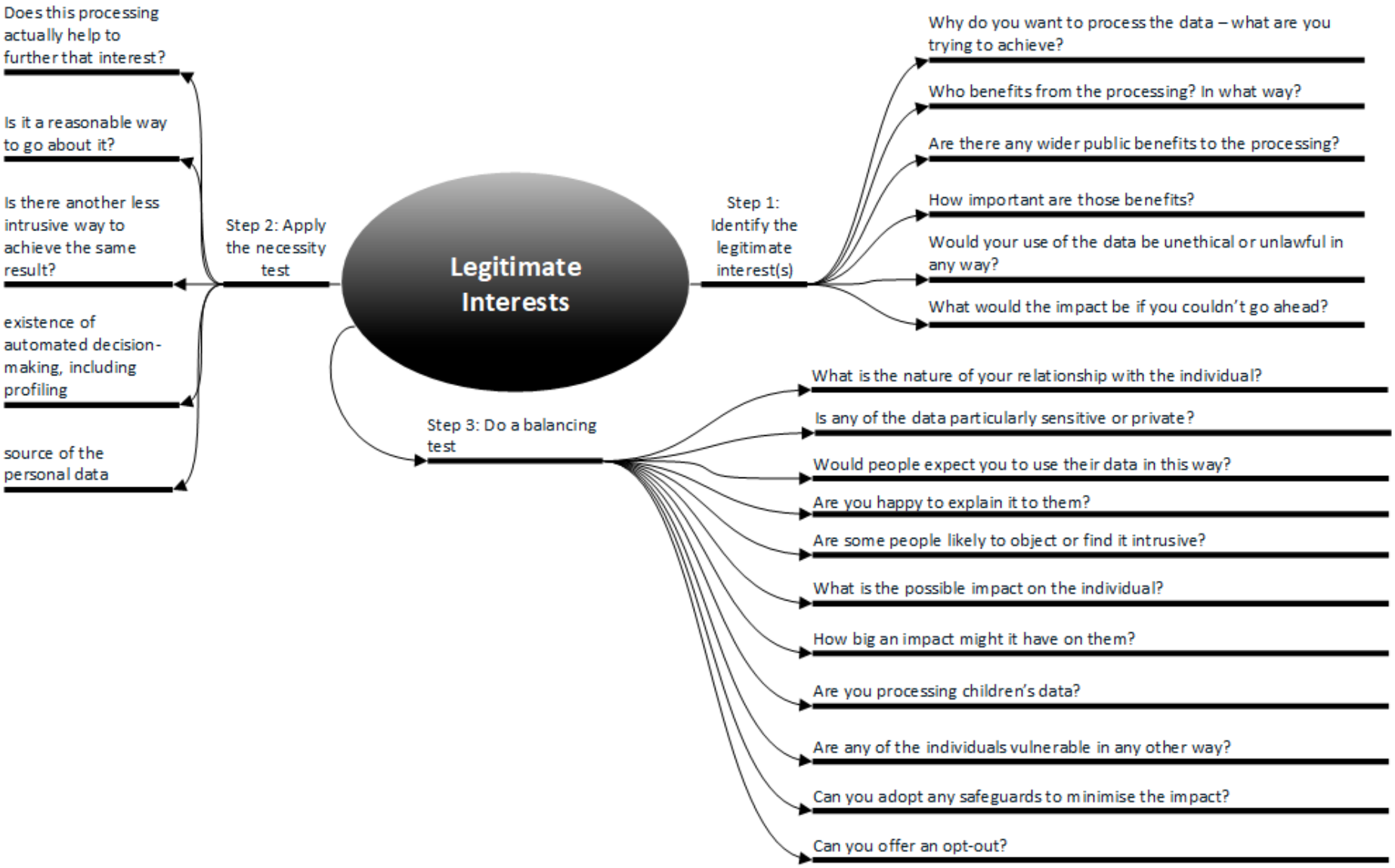
☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.

☐ We keep our LIA under review, and repeat it if circumstances change.

☐ We include information about our legitimate interests in our privacy information.

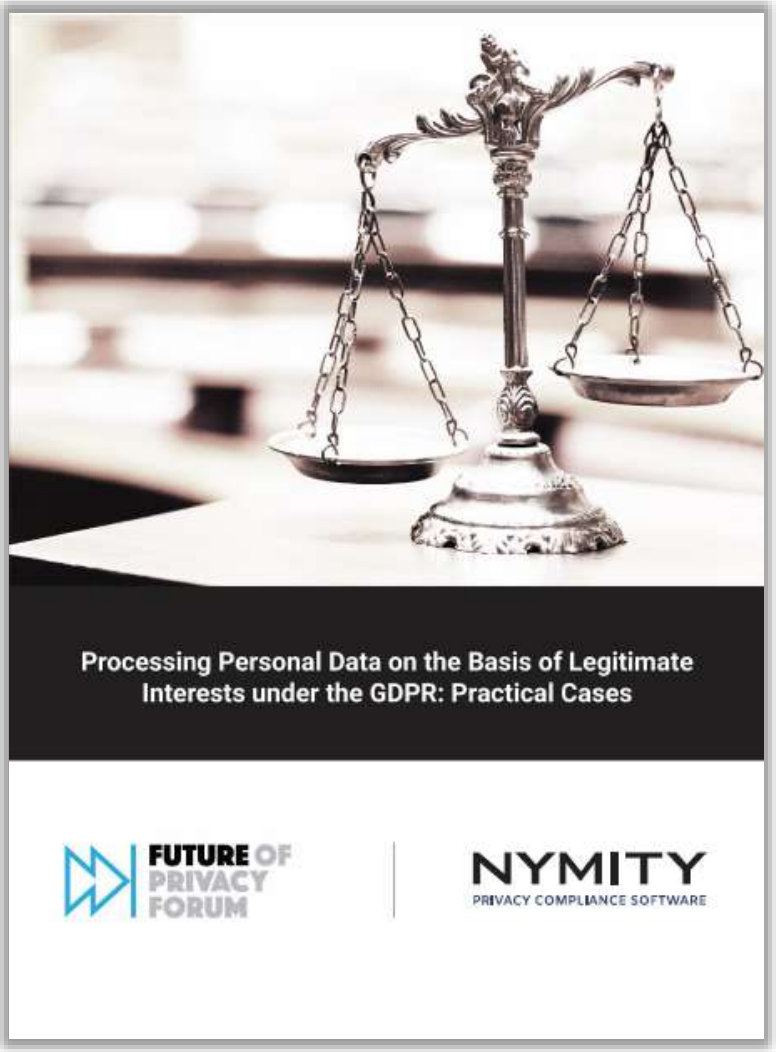
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/

68 Схема проведения Legitimate Interests Assessment



https://wadiff-consulting.co.uk/2018/01/08/legitimate-interest-3-part-test/

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



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

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

https://info.nymity.com/hubfs/Landing%20Pages/Nymity%20FPF%20-%20Legitimate%20Interests%20Report/Deciphering_Legitimate_Interests_Under_the_GDPR.pdf

Руководство от DPN по использованию Legitimate Interests и проведению LIA



Understanding what Legitimate Interests are

Key definitions

The Lawful Basis for processing under the GDPR

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

Identifying areas of processing where Legitimate Interests may apply

How Legitimate Interests might apply

Case studies & examples of where Legitimate Interests may apply

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

Identifying a Legitimate Interest

The 'necessity test'

The 'balancing test'

Transparency and the consumer

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

Appendices:

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

Appendix B – Legitimate Interests Assessment Template

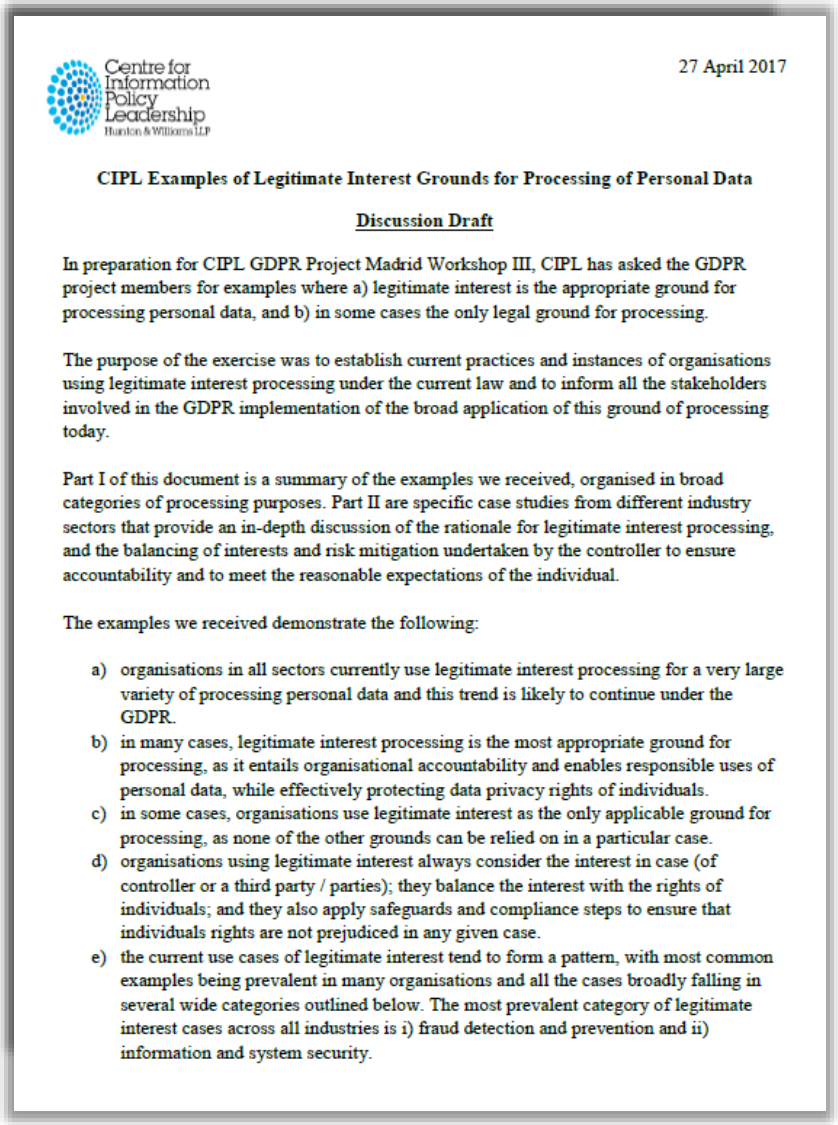
Appendix C - Legitimate Interests Assessment Example

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

Appendix E – Glossary of terms

https://www.fairtrade.org.uk/~/media/FairtradeUK/Resources%20Library/Data%20Protection%20Network%20-%20Guidance%20on%20the%20use%20of%20legitimate%20interest.pdf

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



Centre for Information Policy Leadership
Hunton & Williams LLP

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.

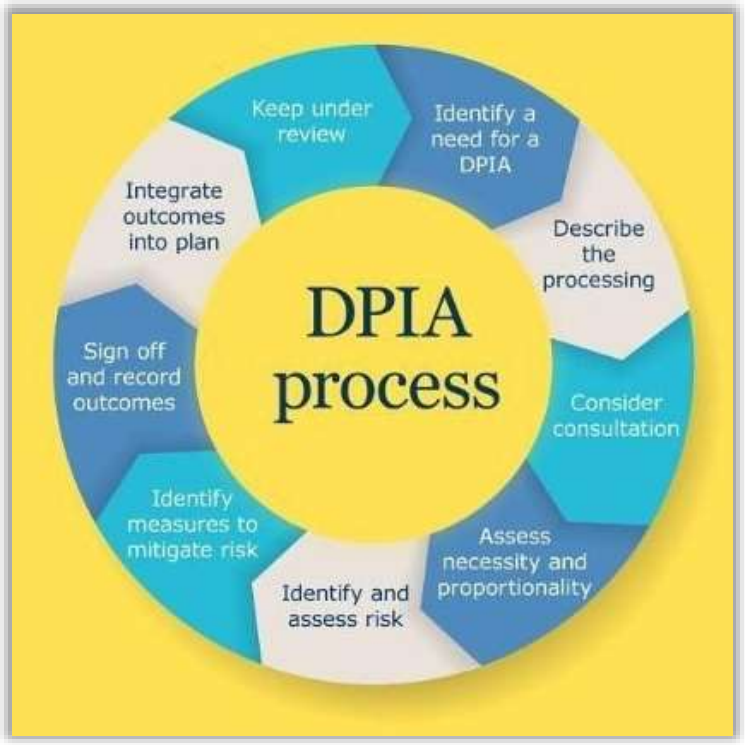
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_27_april_2017.pdf

Data Protection Impact Assessment



К оглавлению

Руководство от ICO по проведению Data protection impact assessments (DPIA)

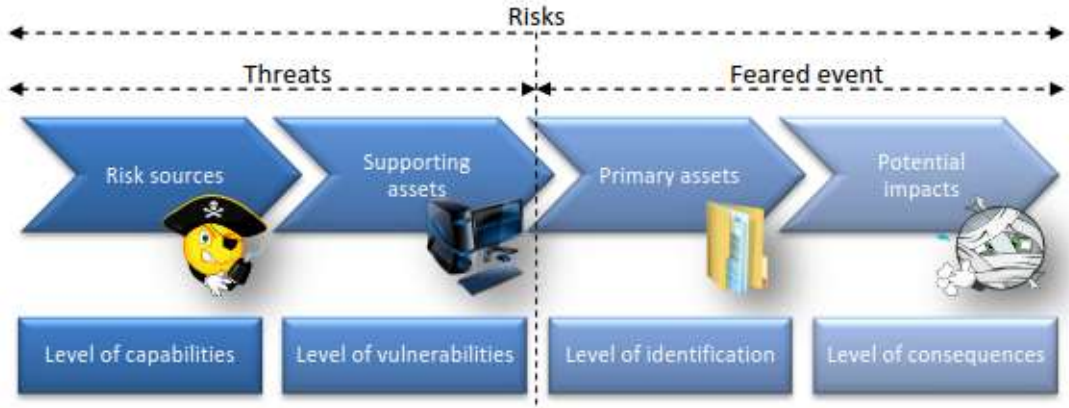


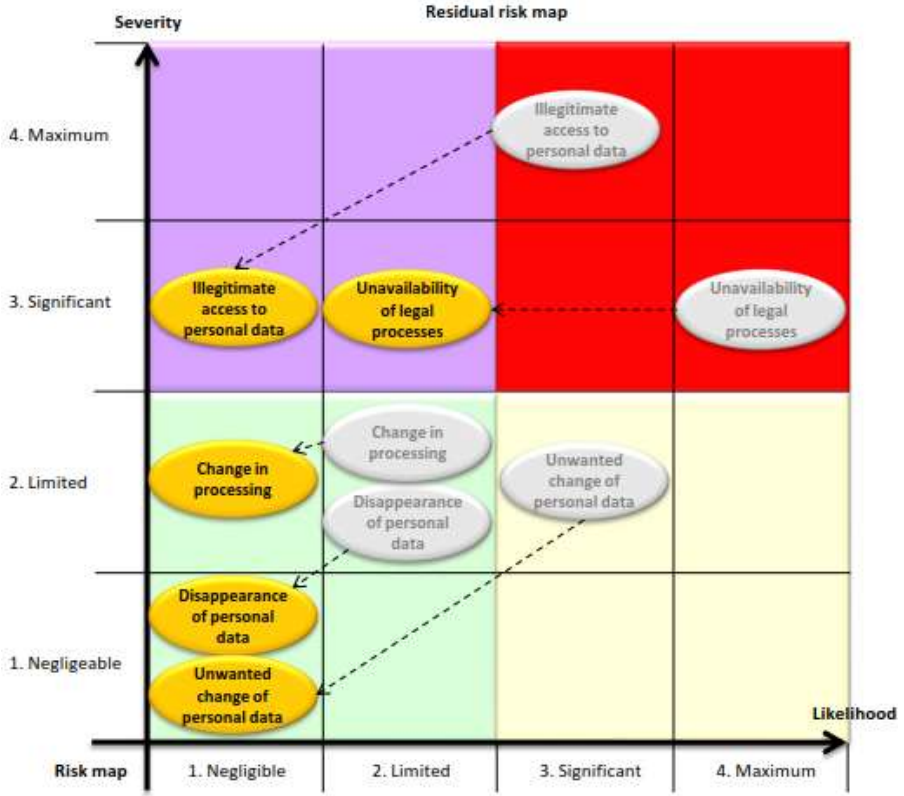
Severity of impact		Likelihood of harm: Remote	Likelihood of harm: Reasonable possibility	Likelihood of harm: More likely than not
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

Руководство от CNIL по методологии управления Privacy-рисками

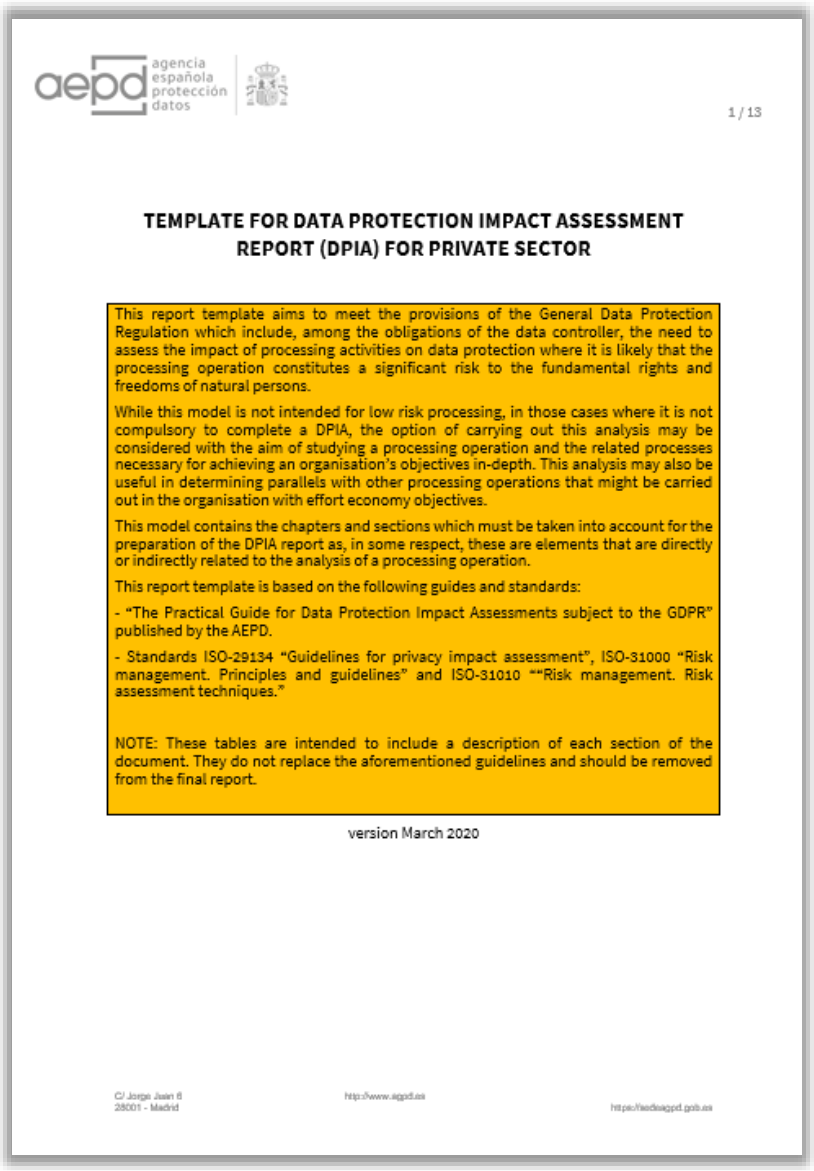






https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

75 Пример реализации DPIA от AEPD для частного сектора



aepd agencia española protección datos

TEMPLATE FOR DATA PROTECTION IMPACT ASSESSMENT REPORT (DPIA) FOR PRIVATE SECTOR

This report template aims to meet the provisions of the General Data Protection Regulation which include, among the obligations of the data controller, the need to assess the impact of processing activities on data protection where it is likely that the processing operation constitutes a significant risk to the fundamental rights and freedoms of natural persons.

While this model is not intended for low risk processing, in those cases where it is not compulsory to complete a DPIA, the option of carrying out this analysis may be considered with the aim of studying a processing operation and the related processes necessary for achieving an organisation's objectives in-depth. This analysis may also be useful in determining parallels with other processing operations that might be carried out in the organisation with effort economy objectives.

This model contains the chapters and sections which must be taken into account for the preparation of the DPIA report as, in some respect, these are elements that are directly or indirectly related to the analysis of a processing operation.

This report template is based on the following guides and standards:

- "The Practical Guide for Data Protection Impact Assessments subject to the GDPR" published by the AEPD.

- Standards ISO-29134 "Guidelines for privacy impact assessment", ISO-31000 "Risk management. Principles and guidelines" and ISO-31010 ""Risk management. Risk assessment techniques."

NOTE: These tables are intended to include a description of each section of the document. They do not replace the aforementioned guidelines and should be removed from the final report.

version March 2020

I. EXECUTIVE SUMMARY

II. TABLE OF CONTENTS

III. PURPOSE OF THE PROCESSING OPERATION
Date of preparation of the DPIA
Name and Description of Processor
Categories of Data
Identification of the Data Controller as per GDPR
Identification of third parties involved in processing
Internal context of the processing operation in the organisation
External context of the organisation and the processing operation

IV. LAWFULNESS OF PROCESSING AND REGULATORY COMPLIANCE

V. DPIA METHODOLOGY
Parties involved in the completion of the DPIA
Guidelines, tools, methodologies, standards and rulings used in the evaluation
Scope and limits of the DPIA: Identify what remains outside the scope of the assessment

VI. ANALYSIS OF THE PROCESSING OPERATION

VII. ANALYSIS OF THE OBLIGATION TO COMPLETE A DPIA: RISK ASSESSMENT
Inclusion of processing operation in the list of exempt processing operations
Analysis of obligation to complete DPIA for the processing operation
Assessment of level of risk

VIII. ANALYSIS OF THE NEED FOR THE PROCESSING OPERATION
Benefits for data subjects
Benefits for the entity
Alternatives to the processing operation and why they were not chosen

IX. MEASURES TO REDUCE THE RISK
Optimising the processing operation
Privacy by design and default (PBDD) measures
Accountability measures
Security Measures

X. RISK-BENEFIT ANALYSIS

XI. ACTION PLAN

XII. CONCLUSIONS AND RECOMMENDATIONS

XIII. APPENDICES

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

76 Обзор Fieldfisher национальных «черных списков» DPIA



Country	Large-scale processing	New tech	Automated decision-making	Profiling and evaluation	Location data and tracking	Combining and matching data	Employee monitoring	Public surveillance	"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.

https://www.fieldfisher.com/en/services/technology-outsourcing-and-privacy/privacy-security-and-information/privacy-security-and-information-law-blog/data-protection-impact-assessments-%E2%80%93-what,-when-an

77 DPIA в отношении Microsoft Office ProPlus



PRIVACY COMPANY

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.

https://www.privacycompany.eu/en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise/

Управление Data Breach



К оглавлению

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

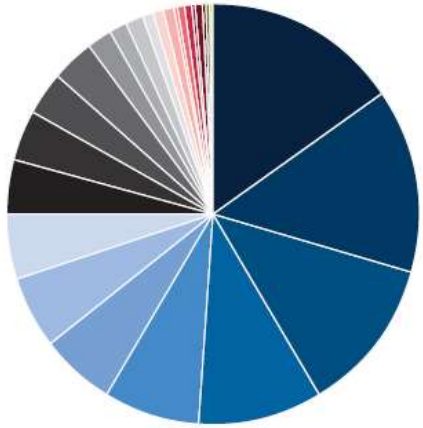
Total number of personal data breaches notified per jurisdiction for the period from 25 May 2018 to 27 January 2020 inclusive*



*Not all of the countries covered by this report make breach notification statistics publicly available and many only provided data for part of the period covered by this report. We have therefore had to extrapolate the data to cover the full period. It is also possible that some of the breaches reported relate to the regime pre-dating GDPR.

**Germany has 16 different State data protection supervisory authorities plus a federal supervisory authority. The supervisory authorities for Baden-Wuertemberg, Mecklenburg Western Pomerania, Saxony and Saxony-Anhalt either provided incomplete data or no data so we have extrapolated data for these States based on the data provided by

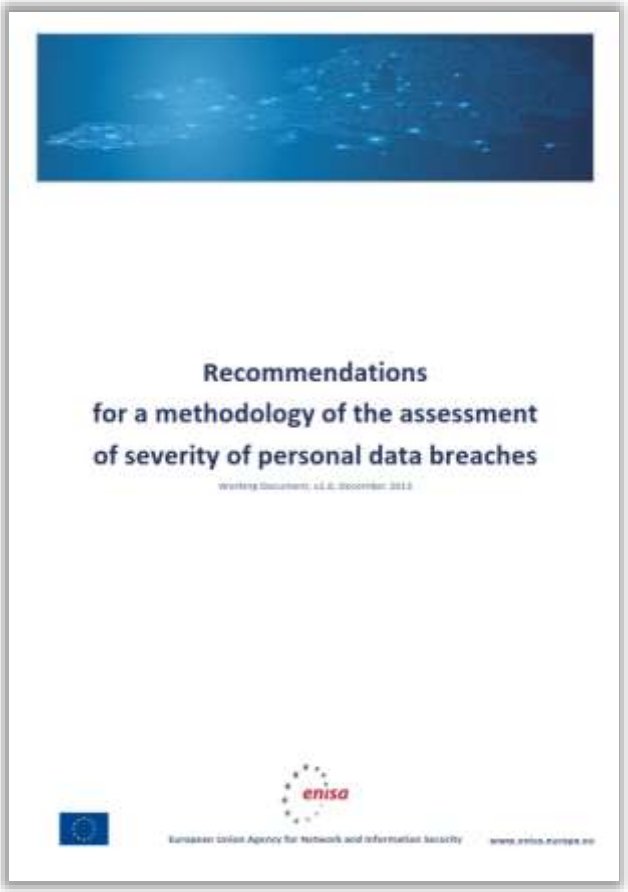
Per capita country ranking of breach notifications*	Number of data breaches per 100,000 people for the period 28 January 2019 to 27 January 2020 inclusive	Change compared to last year's ranking
Netherlands	147.2	0
Ireland	132.52	0
Denmark	115.43	0
Iceland	91.15	+9
Finland	71.11	-1
Luxembourg	56.97	+1
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)

https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/

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



Definition of severity level

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

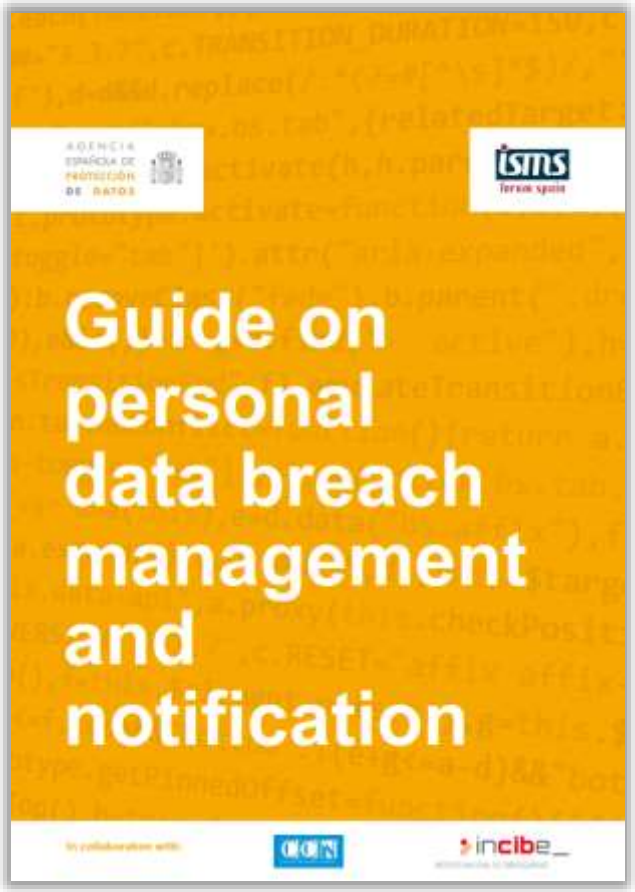
$$SE = DPC \times EI + CB$$

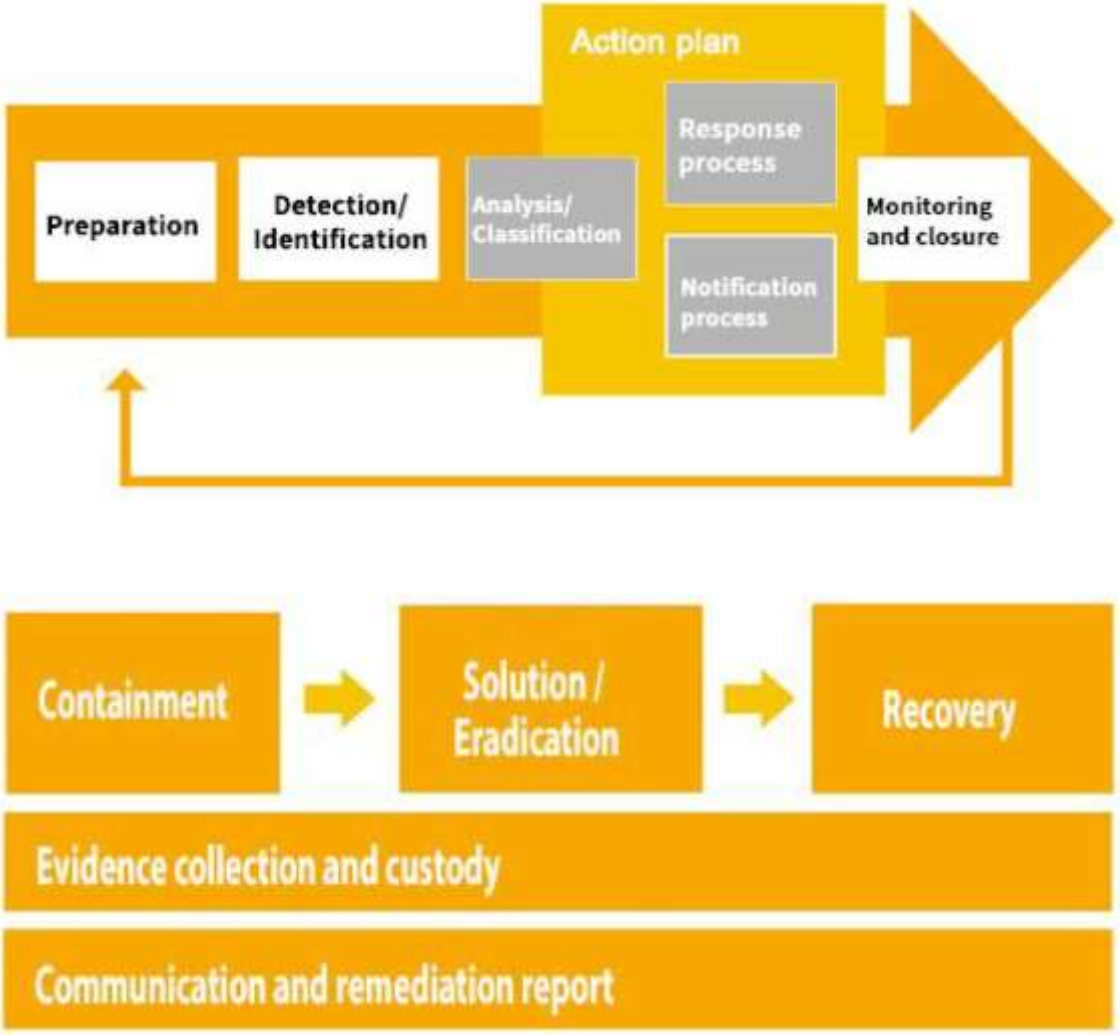
The final score shows the level of severity of a certain breach, taking into account the impact to the individuals[8].

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

https://www.enisa.europa.eu/publications/dbn-severity

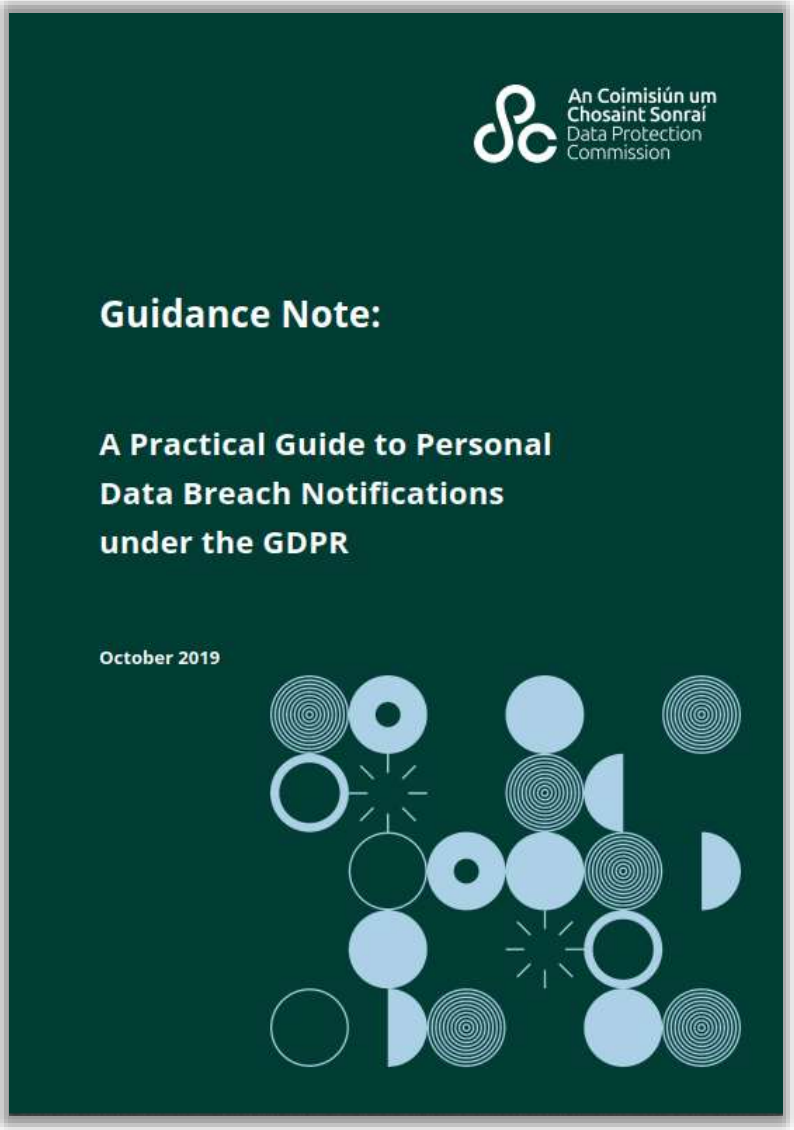
Руководство от AEPD по управлению нарушениями безопасности данных и сообщениями об этом





https://www.aepd.es/media/guias/Guide-on-personal-data-breach.pdf

Практическое руководство от DCP по уведомлениям о нарушениях безопасности персональных данных



Ирландский надзорный орган DCP (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.

https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

Автоматизация Privacy и Data Protection



К оглавлению

84 Website Evidence Collector от EDPS



European Data Protection Supervisor

Бесплатное ПО для автоматизации проверки веб-сайтов, которое собирает информацию об обработке персональных данных, таких как файлы cookie или передачу данных третьим сторонам при посещении сайта. Собранные сведения, структурированные в машиночитаемом формате, позволяют администраторам веб-сайтов, DPO и конечным пользователям лучше понять, какая информация передается и хранится во время посещения веб-сайта.

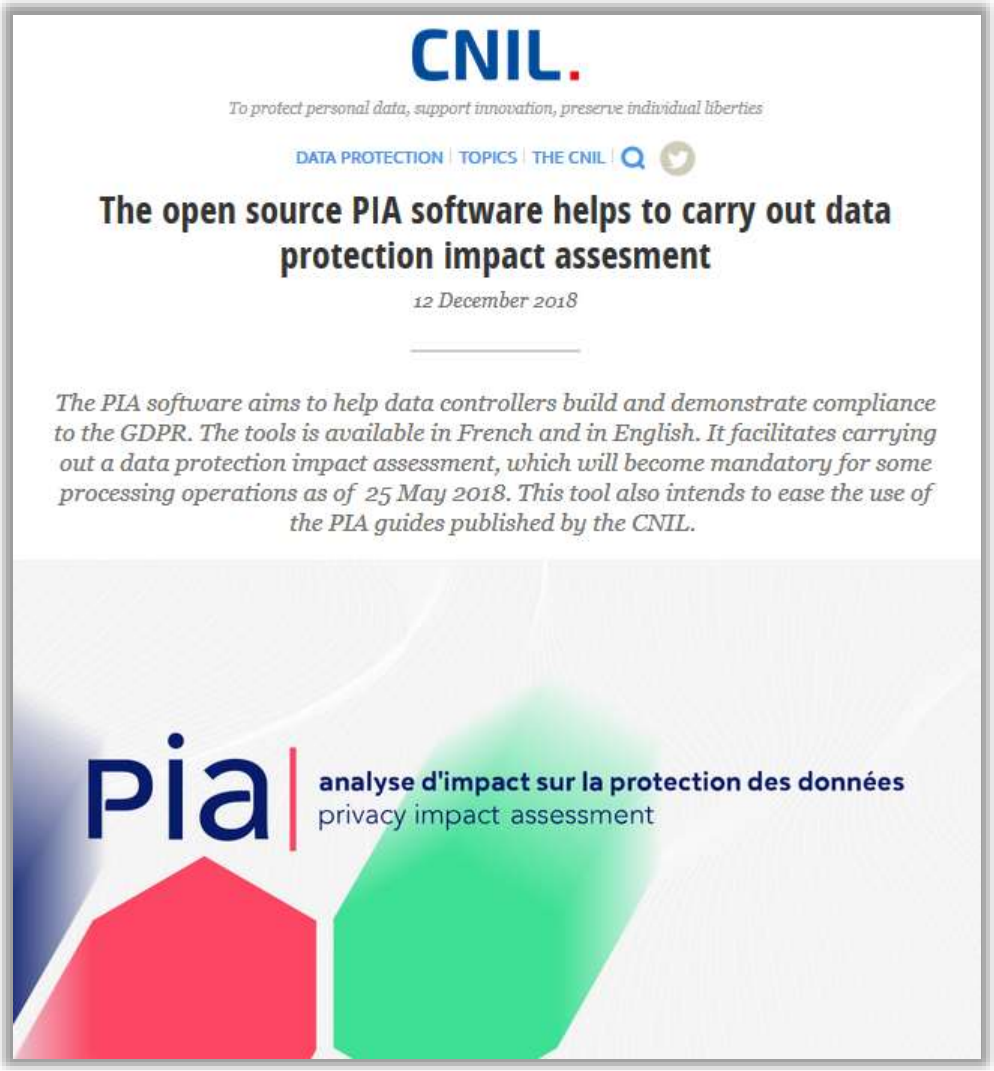
Run Website Evidence Collection

```
links:
  count: 8
  entries:
    - edps.europa.eu
    - twitter.com
    - www.linkedin.com
    - www.youtube.com
    - www.europarl.europa.eu
    - forumti.pl
    - fra.europa.eu
    - edpb.europa.eu

user@linux :~$
```

https://edps.europa.eu/press-publications/edps-inspection-software_en

85 Обзор CNIL по открытому ПО для осуществления DPIA

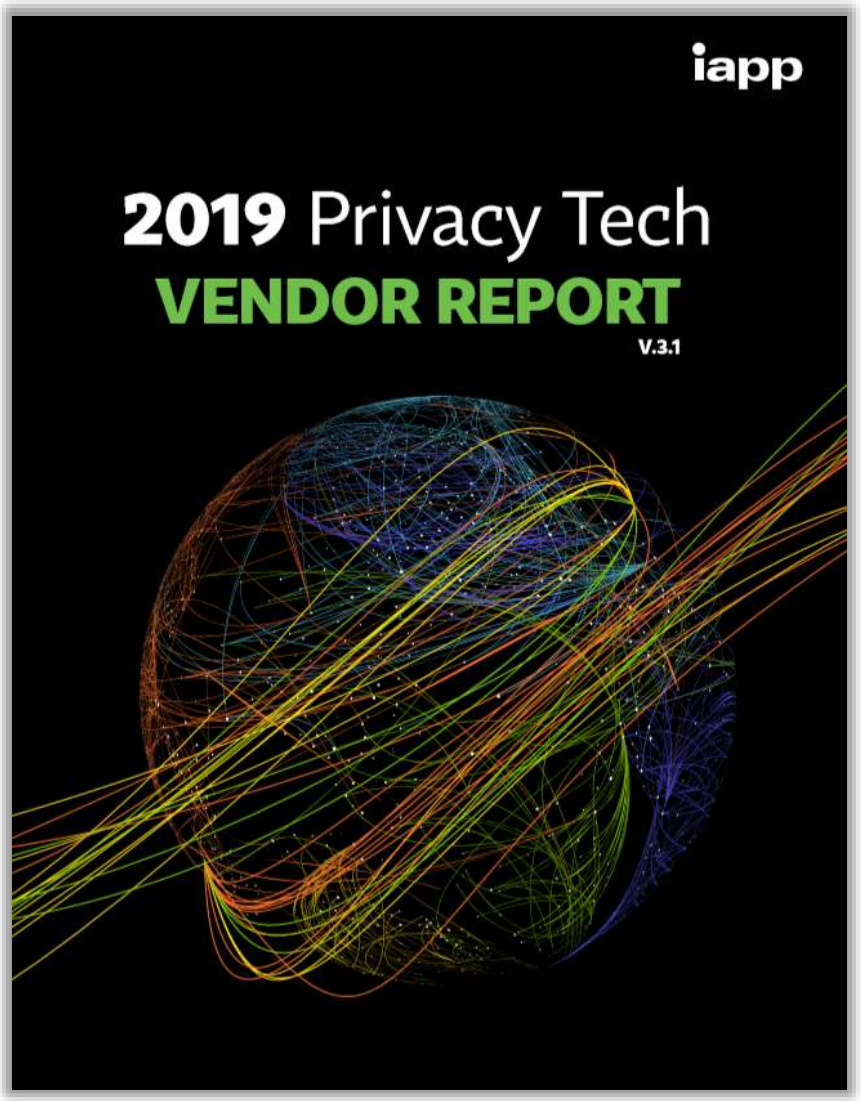


Commission nationale de l'informatique et des libertés

Французский надзорный орган CNIL опубликовал обзор открытого программного обеспечения, облегчающего проведение data protection impact assessment (DPIA) согласно статье 35 GDPR.

https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

86 Privacy Tech Vendor Report от IAPP



International Association of Privacy Professionals

Удобный обзор и классификация Privacy Tech по различному функционалу, а также описание текущего состояния рынка:

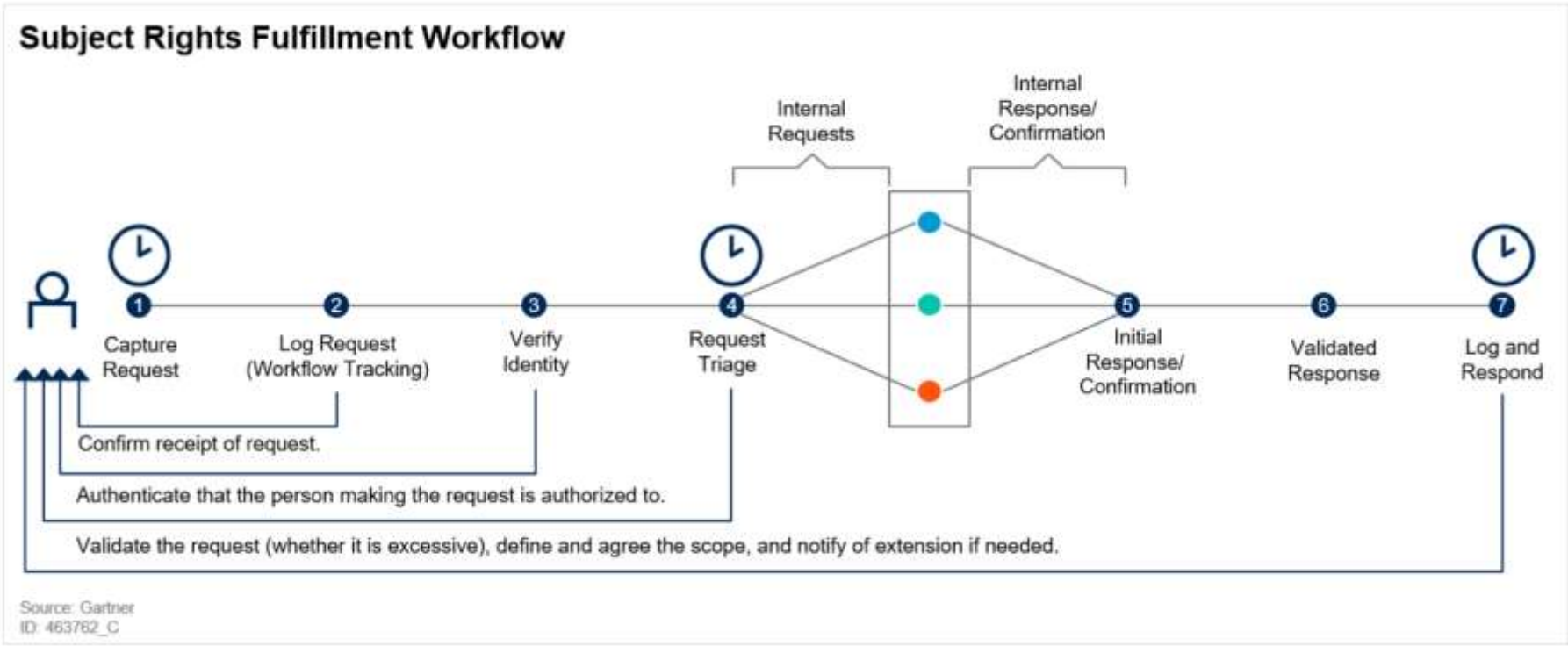
- Privacy Program Management;
- Assessment managers;
- Consent managers;
- Data mapping solutions;
- Incident response solutions;
- Privacy information managers;
- Website scanning;
- Enterprise Privacy Management;
- Activity monitoring;
- Data discovery;
- De-identification/pseudonymity;
- Enterprise communications.

https://iapp.org/media/pdf/resource_center/2019TechVendorReport.pdf

Обзор Forrester по решениям для автоматизации управления комплаенсом в сфере защиты данных



Обзор Gartner по автоматизированным решениям в сфере реализации прав субъектов







https://www.gartner.com/doc/reprints?id=1-1YIGL0C8&ct=200227&st=sb

OneTrust – обзор решений

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

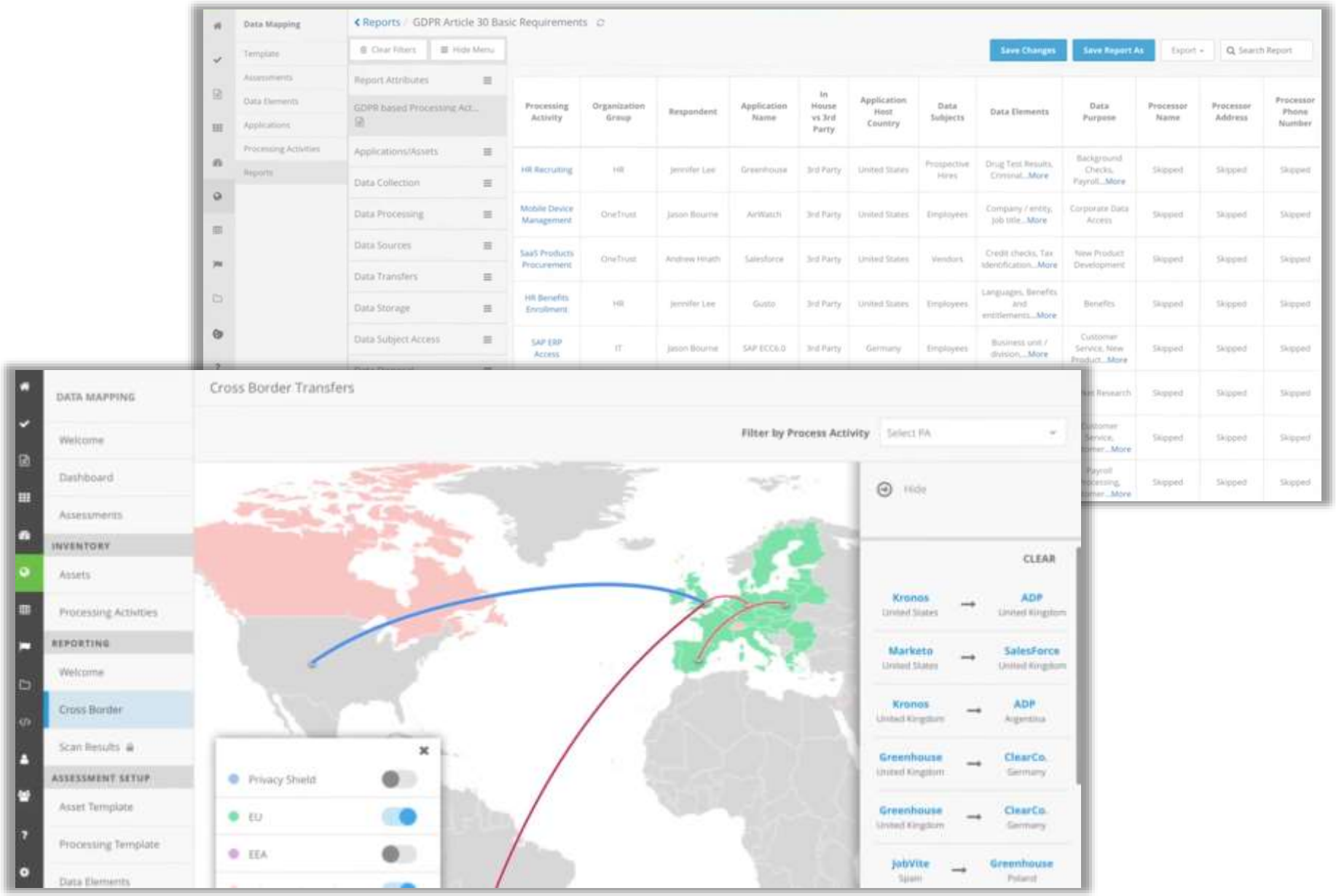
Marketing & Web Compliance

- Data Subject Rights Management
- Website Compliance Scanning
- Cookie Consent Management
- Universal Consent Management
- Enterprise Preference Center
- IAB Publisher Consent
- Mobile App Consent

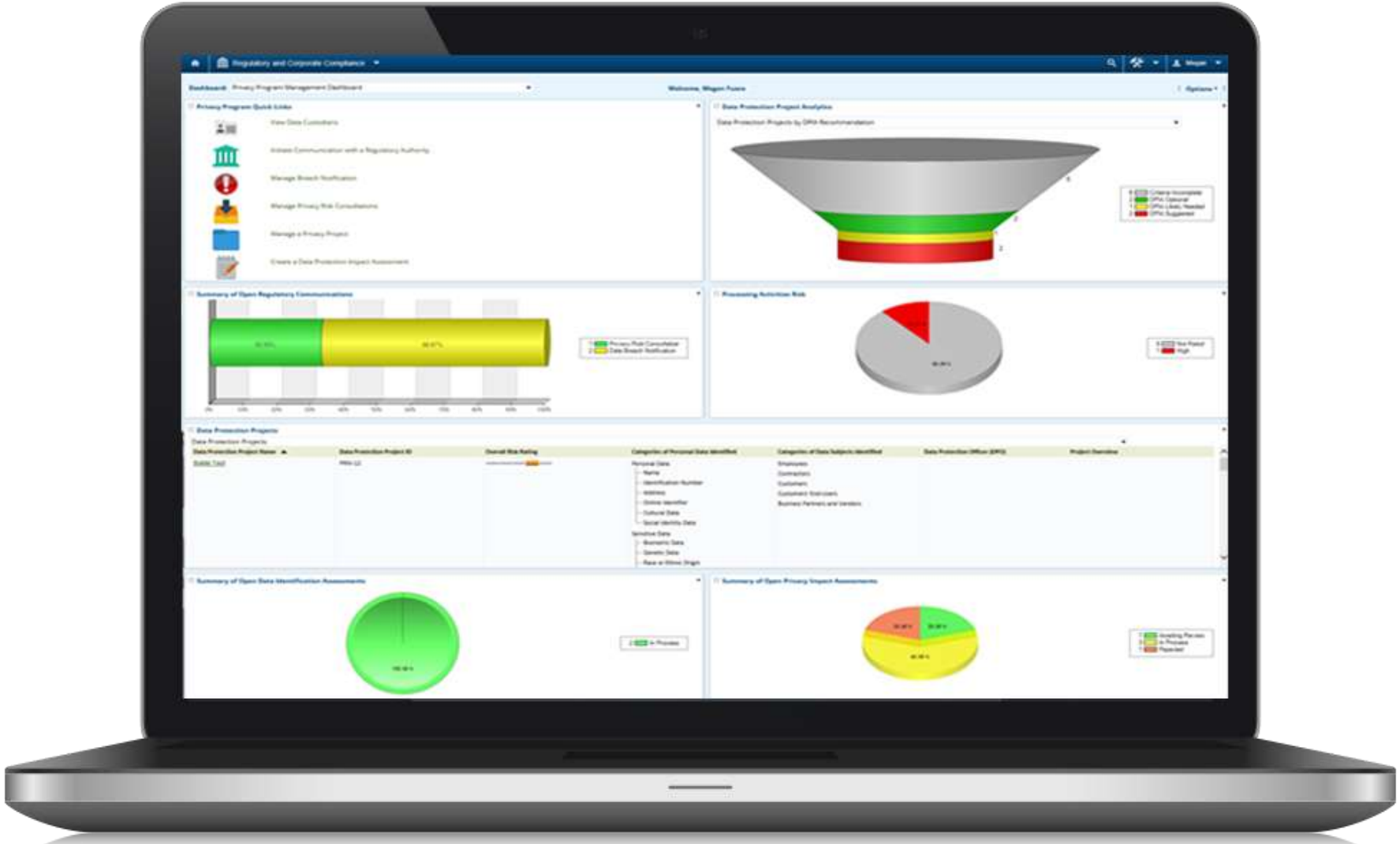
GDPR & Global Privacy Solutions

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

90 OneTrust – Data Mapping Automation



RSA Archer Privacy Program Management

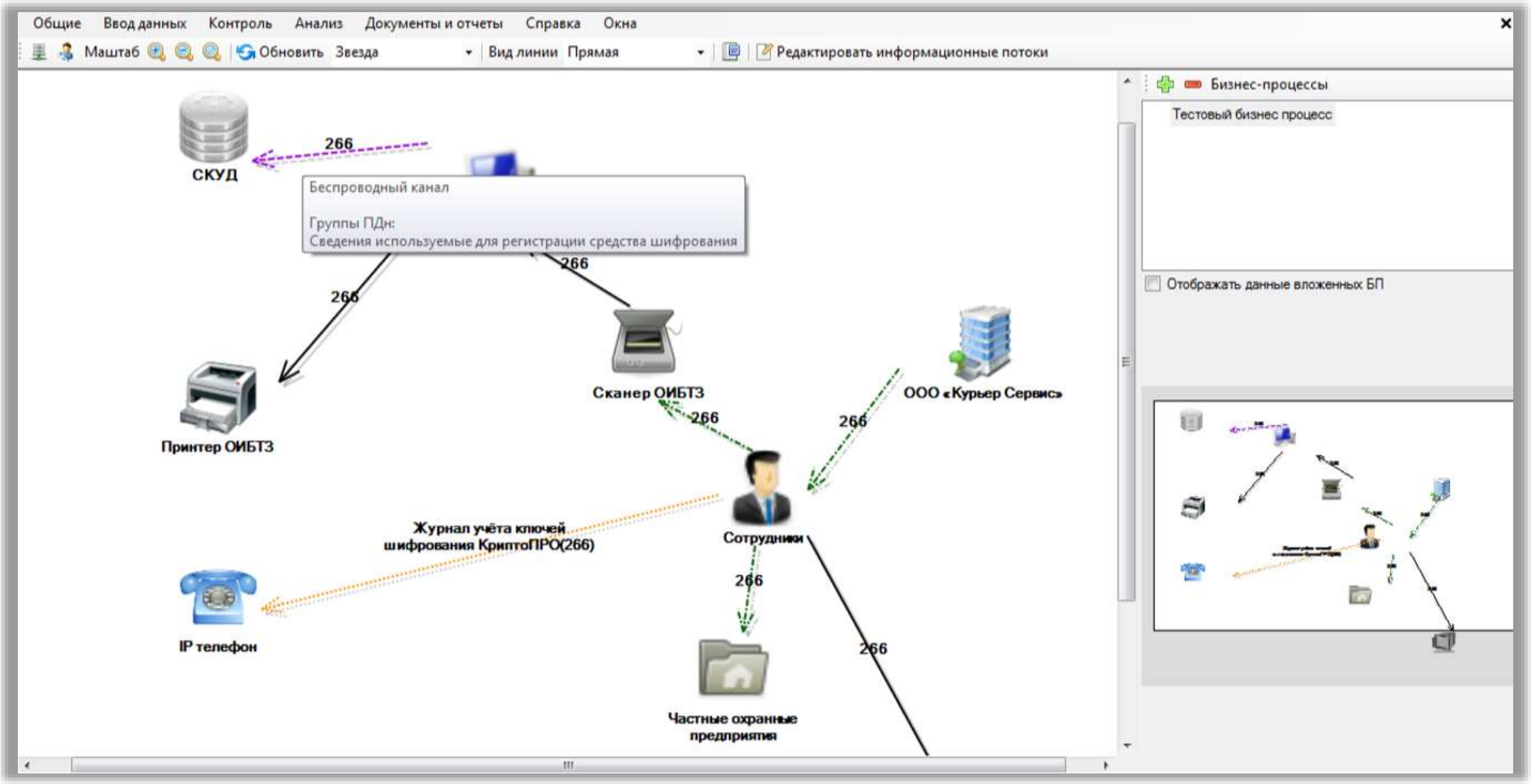


Интеграция между OneTrust и RSA Archer



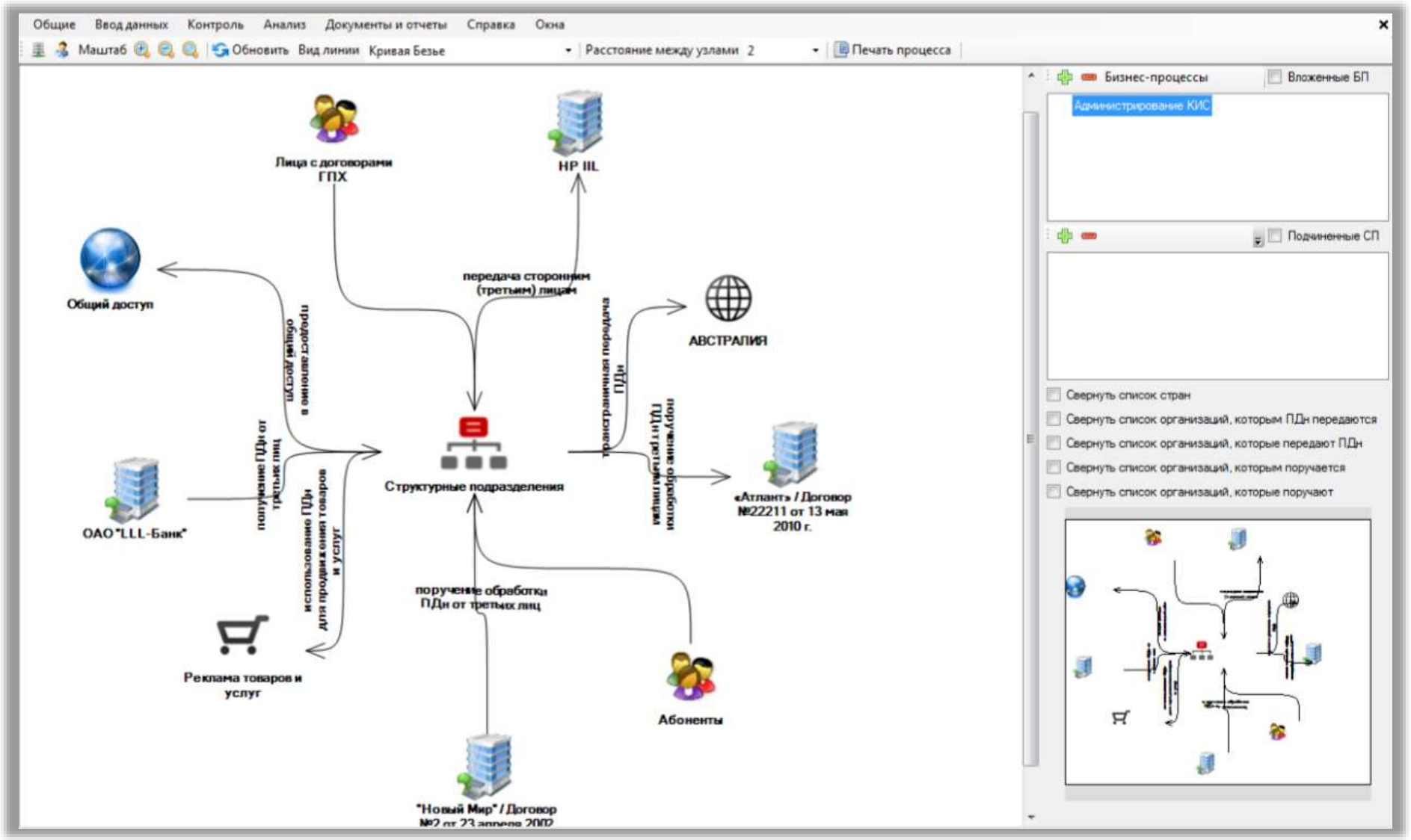
https://www.onetrust.com/onetrust-rsa-partnership/

Privacy-SPS (IRADD) - Пример интерфейса «Визуализация информационных потоков»

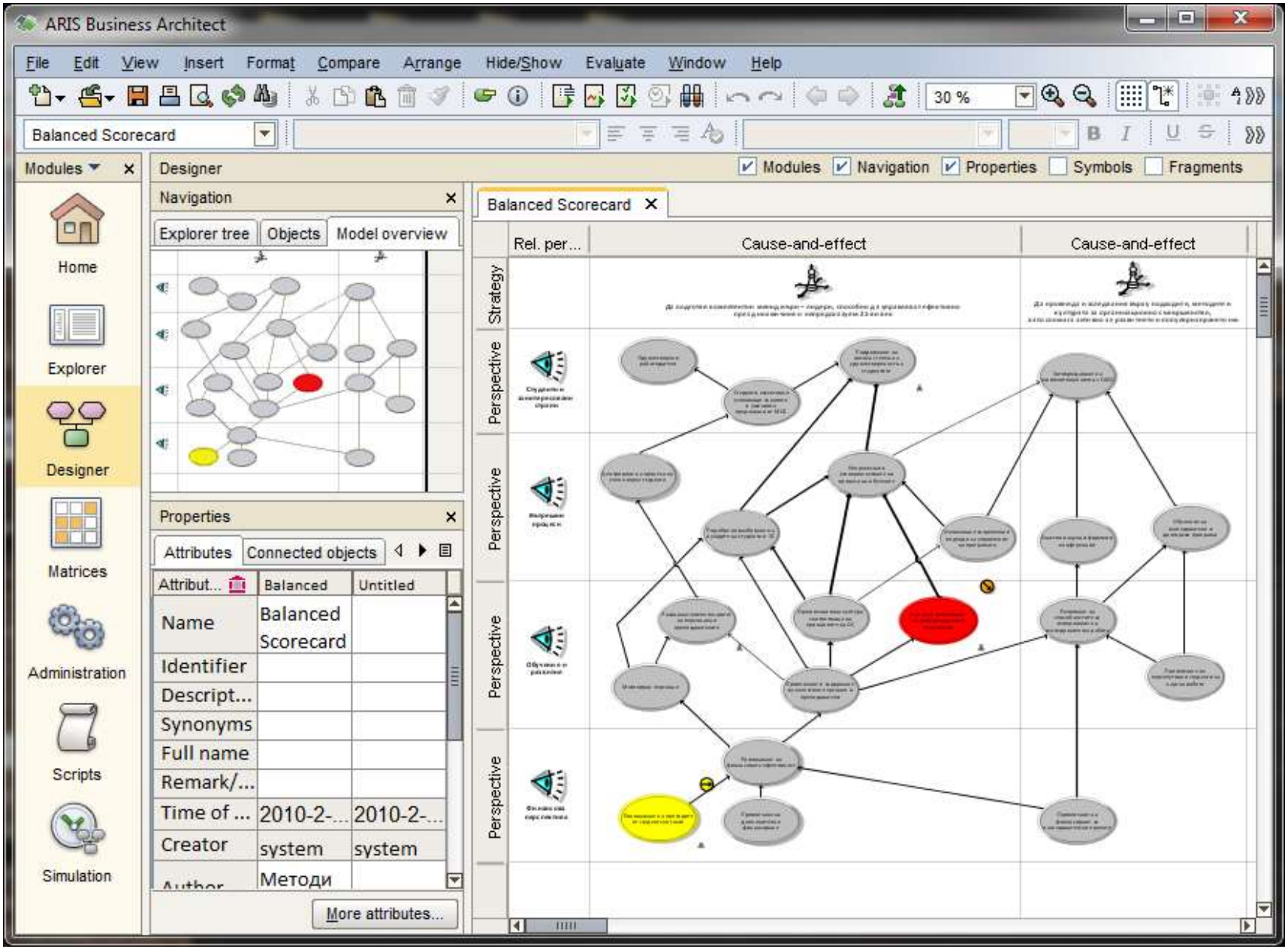


Privacy-SPS включено в Единый реестр российских программ для электронных вычислительных машин и баз данных - https://reestr.minsvyaz.ru/reestr/73559/

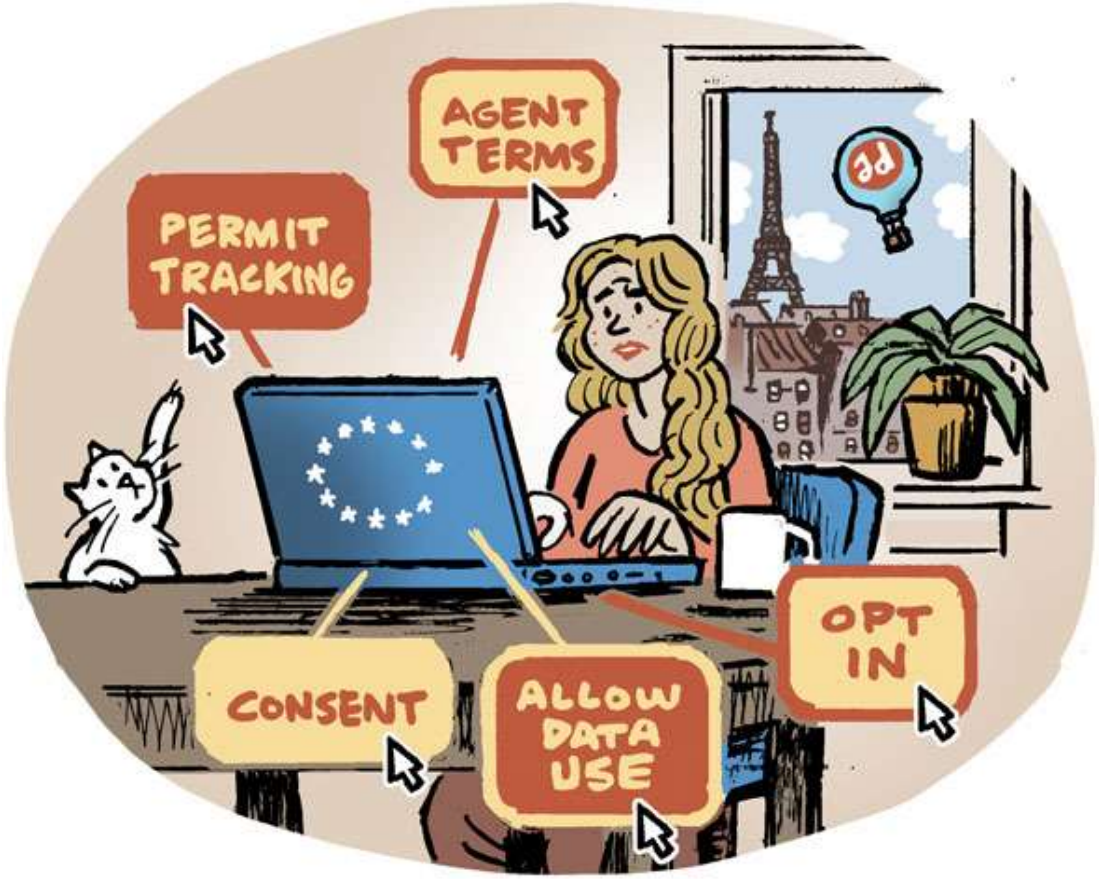
Privacy-SPS - Пример интерфейса «Визуализация процессов обработки ПДн»



ARIS (Architecture of Integrated Information Systems)

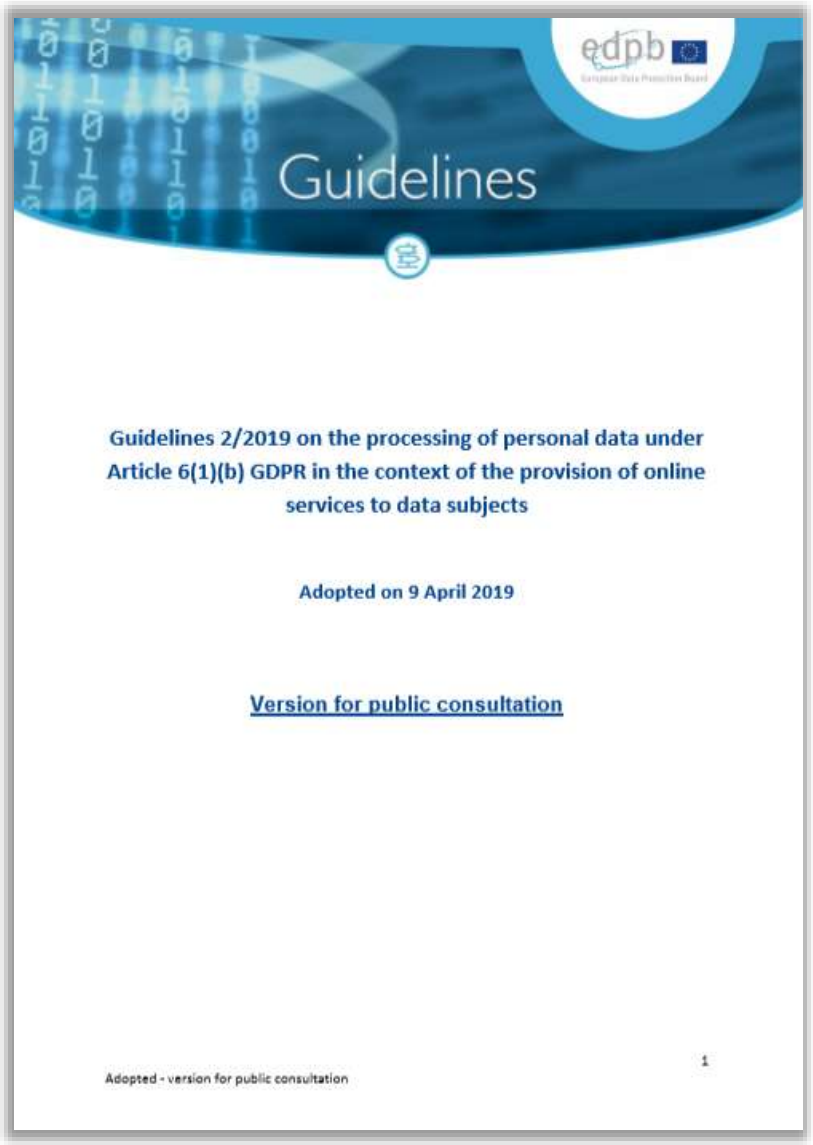


Взаимодействие с пользователями сайтов и приложений



К оглавлению

Руководство EDPB по обработке персональных данных при предоставлении онлайн-услуг субъектам



Европейский совет по защите данных (European Data Protection Board) принял проект руководства 2/2019 по применимости ст.6(1)(b) GDPR в контексте предоставления онлайн-услуг субъектам данных.

Это руководство призвано помочь в определении правового основания обработки персональных данных в контексте заключаемых с субъектами данных контрактов на оказание им онлайн-услуг, независимо способа оплаты данных услуг. В руководстве изложены квалифицирующие признаки правомерной обработки персональных данных в соответствии со ст.6(1)(b) GDPR и рассмотрена концепция «необходимости» в том виде, в каком она применима к исполнению контракта.

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf

Тезисы руководства EDPB по обработке данных при предоставлении онлайн-услуг субъектам

- ✓ После расторжения контракта обычно несправедливо переходить на другое легальное основание (п. 41).
- ✓ Действия, связанные с контрактом после его расторжения (возврат оплаты и т.п.) тоже могут быть основаны на статье 6(1)(b). (п. 42, 44).
- ✓ Сбор детальной информации о пользователе для улучшения сервиса должен осуществляться на иных основаниях: легитимный интерес, согласие (п. 48, 49).
- ✓ Мониторинг и профилирование клиентов в целях предотвращения мошенничества выходят за рамки контракта, как основание используется легитимный интерес или правовое обязательство (п. 50).
- ✓ Обычно контракт с клиентом не является основанием для демонстрации ему таргетированной рекламы. Но если хочется, нужно учесть, что клиент имеет право возражать против прямого маркетинга по статье 21 GDPR (п. 52), учесть требования ePrivacy, мнение по WP171 и WP208 (п. 55).
- ✓ Отслеживание групп пользователей для демонстрации им определенного товара также не является необходимым для исполнения контракта (п. 56).
- ✓ Персональные данные не могут рассматриваться в качестве коммерческого товара (п. 54).
- ✓ Персонализация контента может (но не всегда) быть неотъемлемым и ожидаемым элементом некоторых онлайн-сервисов и, следовательно, может считаться необходимой для выполнения контракта с пользователем сервиса в некоторых случаях (п. 57).

Один из интересных примеров (№ 8):
Онлайн торговая площадка позволяет потенциальным покупателям просматривать и покупать товары. Торговая площадка желает показывать персонализированные предложения по продуктам, основанные на том, какие списки потенциальные покупатели ранее просматривали на платформе для повышения интерактивности. *Эта персонализация не является объективно необходимой для предоставления услуг на рынке. Таким образом, такая обработка персональных данных не может основываться на статье 6(1)(b) в качестве правового основания.*

https://m.facebook.com/groups/gdpr152/permalink/711357612715349/

Руководство ICO по использованию файлов cookie и аналогичных технологий



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.

https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/

100 Руководство AP по использованию файлов cookie



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.

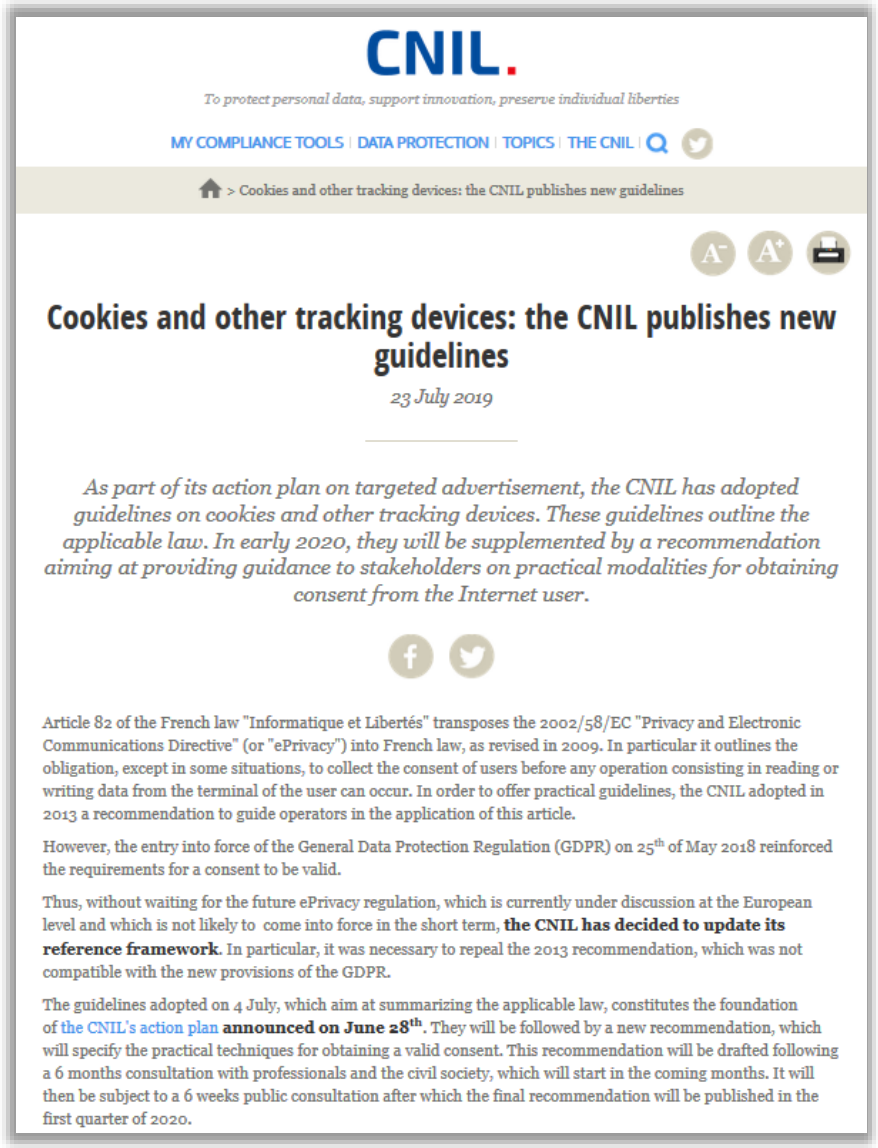
Нидерландский надзорный орган Autoriteit Persoonsgegevens (AP) в марте 2019 года руководство по использованию файлов cookie, согласно которому «стены файлов cookie» (cookie walls) нарушают требования GDPR. Стена файлов cookie - это всплывающее окно на веб-сайте, которое блокирует доступ пользователя 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).

https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies

Руководство CNIL по использованию файлов cookie и иных аналогичных технологий



CNIL.

To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL

> Cookies and other tracking devices: the CNIL publishes new guidelines

Cookies and other tracking devices: the CNIL publishes new guidelines

23 July 2019

As part of its action plan on targeted advertisement, the CNIL has adopted guidelines on cookies and other tracking devices. These guidelines outline the applicable law. In early 2020, they will be supplemented by a recommendation aiming at providing guidance to stakeholders on practical modalities for obtaining consent from the Internet user.

Article 82 of the French law "Informatique et Libertés" transposes the 2002/58/EC "Privacy and Electronic Communications Directive" (or "ePrivacy") into French law, as revised in 2009. In particular it outlines the obligation, except in some situations, to collect the consent of users before any operation consisting in reading or writing data from the terminal of the user can occur. In order to offer practical guidelines, the CNIL adopted in 2013 a recommendation to guide operators in the application of this article.

However, the entry into force of the General Data Protection Regulation (GDPR) on 25th of May 2018 reinforced the requirements for a consent to be valid.

Thus, without waiting for the future ePrivacy regulation, which is currently under discussion at the European level and which is not likely to come into force in the short term, **the CNIL has decided to update its reference framework**. In particular, it was necessary to repeal the 2013 recommendation, which was not compatible with the new provisions of the GDPR.

The guidelines adopted on 4 July, which aim at summarizing the applicable law, constitutes the foundation of the CNIL's action plan **announced on June 28th**. They will be followed by a new recommendation, which will specify the practical techniques for obtaining a valid consent. This recommendation will be drafted following a 6 months consultation with professionals and the civil society, which will start in the coming months. It will then be subject to a 6 weeks public consultation after which the final recommendation will be published in the first quarter of 2020.

Французский надзорный орган Commission nationale de l'informatique et des libertés (CNIL) в июле 2019 года отменил действовавшие с 2013 года рекомендацию по использованию файлов cookie, которая не была совместима с новыми положениями GDPR, и начал процедуру принятия нового руководства, соответствующего требованиям GDPR и будущего регламента ePrivacy.

Теперь прокрутка вниз или пролистывание веб-сайта или приложения больше не может рассматриваться как действительное выражение согласия на использование файлов cookie. Владелец сайта и третьи лица, отслеживающие действия пользователей, должны иметь возможность доказать факт получения пользовательского согласия.

https://www.cnil.fr/en/cookies-and-other-tracking-devices-cnil-publishes-new-guidelines

Руководство CNIL по получению согласий пользователей на использование файлов cookie и аналогичных технологий



Figure 1 - Le détail des finalités est disponible sous un bouton de déroulement que l'utilisateur peut activer sur le premier niveau d'information.



Figure 2 - Le détail des finalités est disponible en cliquant sur un lien hypertexte présent sur le premier niveau d'information

Французский надзорный орган Commission nationale de l'informatique et des libertés (CNIL) начал публичные консультации по проекту своих рекомендаций о получении согласий пользователей сайтов и приложений при использовании cookie-файлов и других технологий слежения. Консультации продлятся до 25.02.2020.

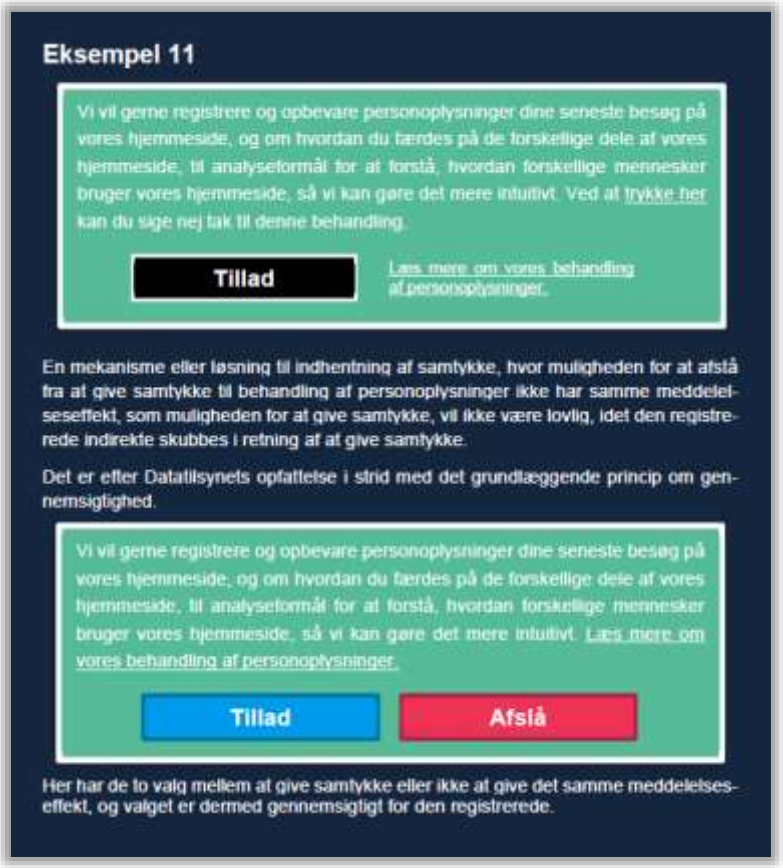
Проект руководства:
https://www.cnil.fr/sites/default/files/atoms/files/projet_de_recommandation_cookies_et_autres_traceurs.pdf

https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-son-projet-de-recommandation-cookies-et-autres-traceurs

Руководство Datatilsynet по обработке персональных данных пользователей веб-сайтов



Датский надзорный орган в сфере персональных данных (Datatilsynet) 17.02.2019 свои рекомендации по обработке персональных данных пользователей веб-сайтов.



https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/feb/nye-retningslinjer-om-behandling-af-personoplysninger-om-hjemmesidebesoegende/

104 Руководство AEPD по использованию файлов cookie



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.

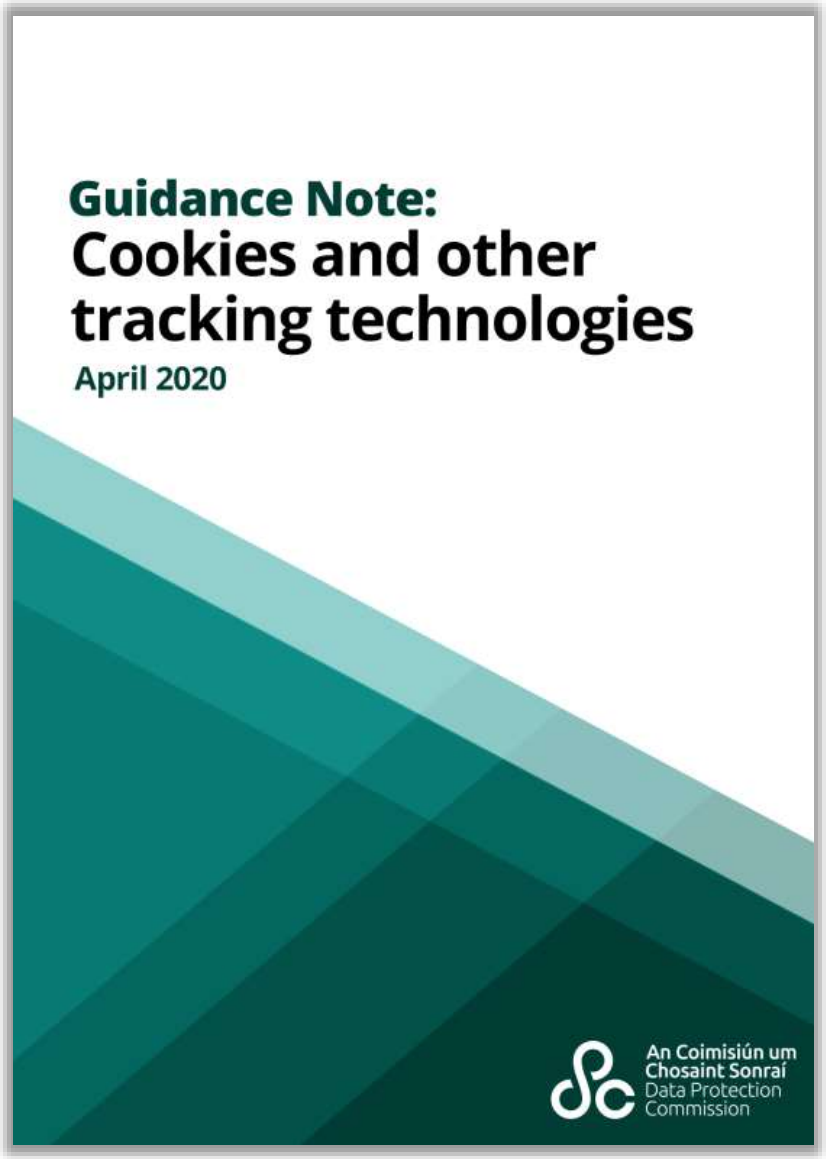
We use both our own and third-party cookies to find out how you use our website and prepare statistical surveys. More information.

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

https://www.aepd.es/sites/default/files/2019-12/guia-cookies-en.pdf

Руководство DPC по использованию файлов cookie и иных аналогичных технологий



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

https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

106 Решение Datatilsynet по делу DMI

Датский надзорный орган в сфере персональных данных (Datatilsynet) 11.02.2020 опубликовал информацию о своем решении в отношении жалобы пользователя сайта Датского Метеорологического Института (DMI) на неправомерную 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 оператора 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.

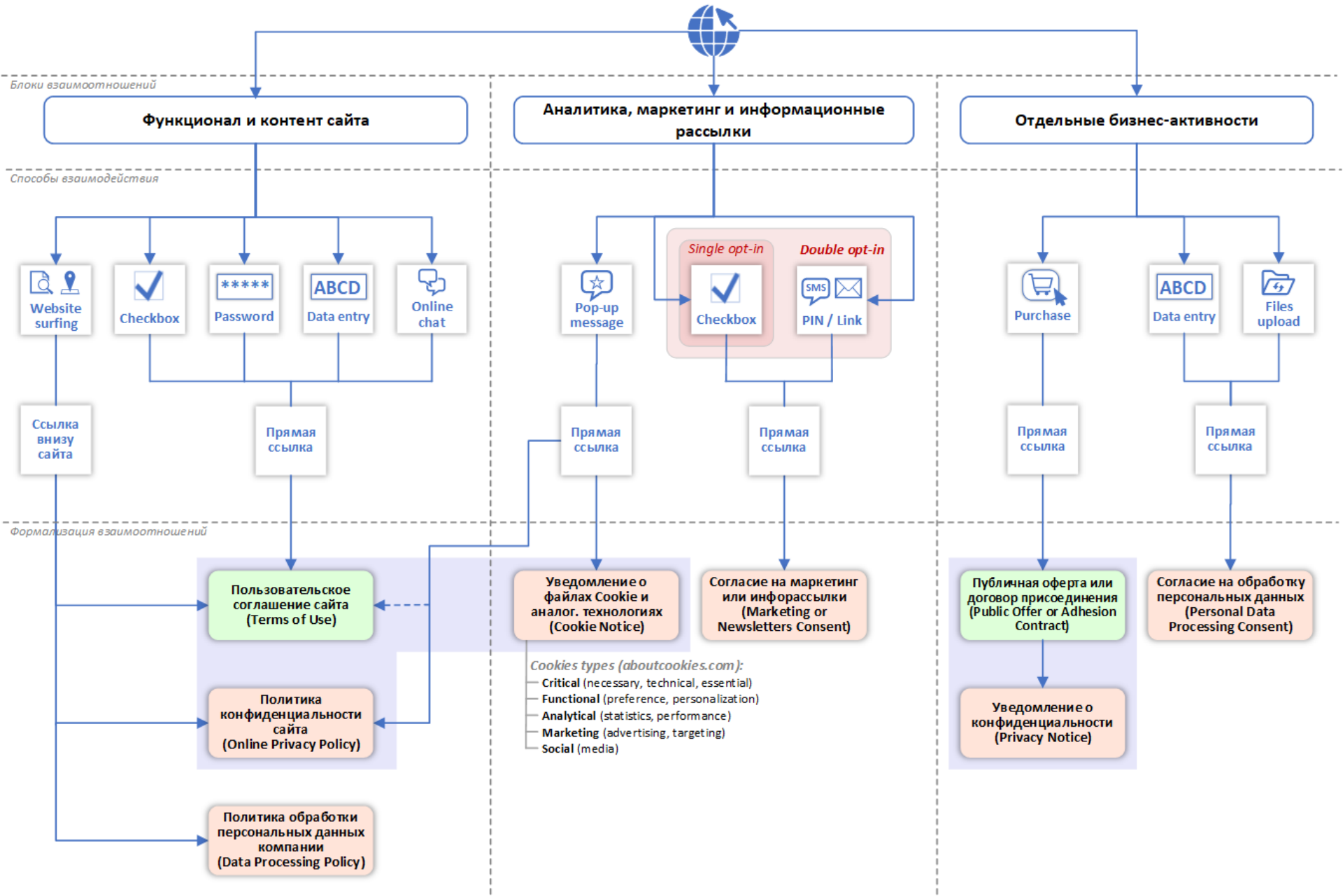
3. Было указано, что субъекты данных должны быть в простой и легко понятной форме осведомлены о контролерах и целях обработки файлов cookie. Так, в описании маркетинговых файлов cookie кратко описывается их поставщик (DoubleClick) и нет достаточно четкой информации о том, что для таких файлов совместными 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.

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/feb/dmis-behandling-af-personoplysninger-om-hjemmesidebesoegende/
https://www.linkedin.com/pulse/danish-dpa-zooms-cookie-consent-banner-design-peeks-bitiukova/

Общий обзор руководств DPA по использованию файлов cookie и аналогичных технологий

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

108 Взаимодействие с субъектами посредством сайтов



Файлы cookies в европейском правовом поле защиты данных



Gottfried Wilhelm Leibniz Universität Hannover

Universitetet I Oslo

Leibniz Universität Hannover

EULISP 2017/2018 – European Legal Informatics Study Programme

MASTER'S THESIS (DOUBLE DEGREE)

COOKIES IN THE EUROPEAN DATA PROTECTION FRAMEWORK

By:

Riccardo Andres Junior Vanzo

Supervisor:

Dr. Marcelo Corrales, LL.M.

Date of submission: September 19th 2018

Deadline for submission: September 20th 2018

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

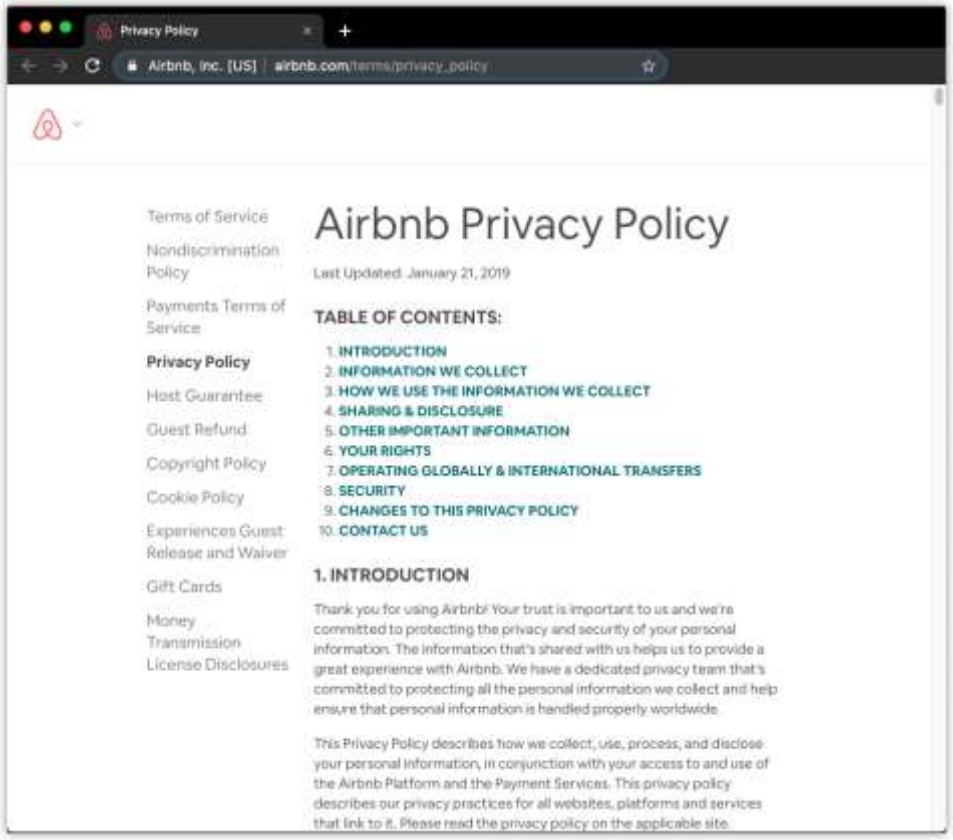
Note: FPC: First Party Cookies, TPC: Third Party Cookies

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

110 Общие советы по написанию Privacy Policy от Emily Gaston



По мнению автора исследования Политика конфиденциальности должна содержать следующие разделы:

- принципы обработки данных;
- категории обрабатываемых данных;
- цели обработки данных;
- правовые основания сбора данных;
- третьи лица, получающие доступ к данным;
- обеспечение конфиденциальности детей;
- права потребителей в отношении данных;
- контактная информация.

https://www.usdigitalpartners.com/how-to-write-a-privacy-policy/

111 Сервисы по предупреждению об использовании cookies



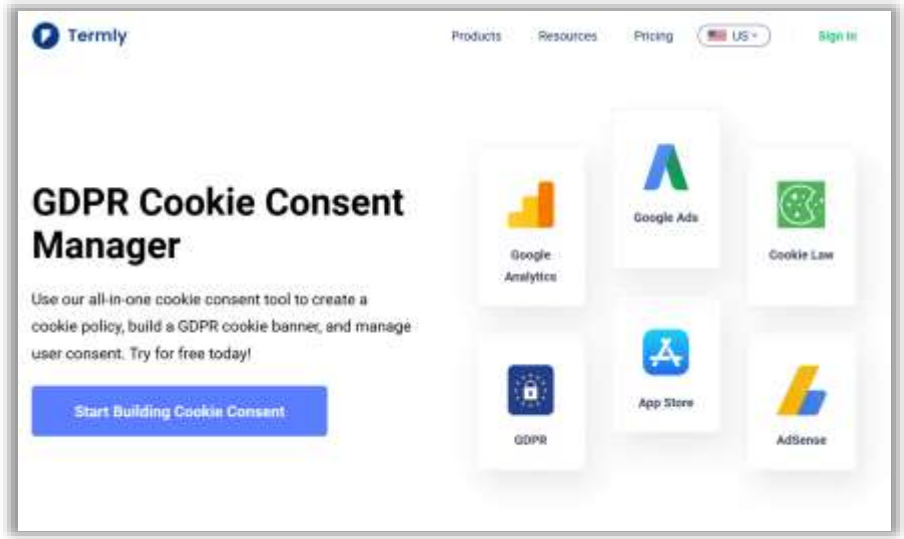
https://www.cookiebot.com/en/



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



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



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

Анализ порочной практики мобильных приложений по сбору данных пользователей

App	Summary of findings
Clue	Sends birth year to **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.

https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

Разъяснение от Datatilsynet об обработке персональных данных при публикация фото людей в Интернете



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.

https://www.datatilsynet.dk/emner/internet-og-apps/billeder-paa-internettet/

Руководство от ENISA по конфиденциальности и защите данных в мобильных приложениях



GDPR PRINCIPLES	INDICATIVE PRIVACY RISKS	INDICATIVE REQUIREMENTS
Lawfulness, fairness and transparency Art.5(1)(a)	Unlawful, excessive and incorrect processing (e.g. due to permissions to unauthorised parties to access personal data through the app).	App providers/developers should make sure that they have a legal basis for the processing of personal data. 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. 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.
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.

https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications

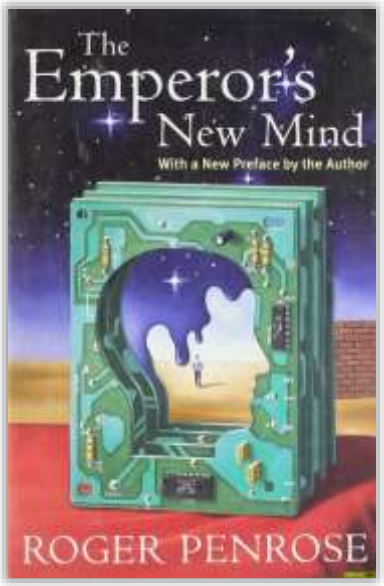
Большие данные, искусственный интеллект и машинное обучение



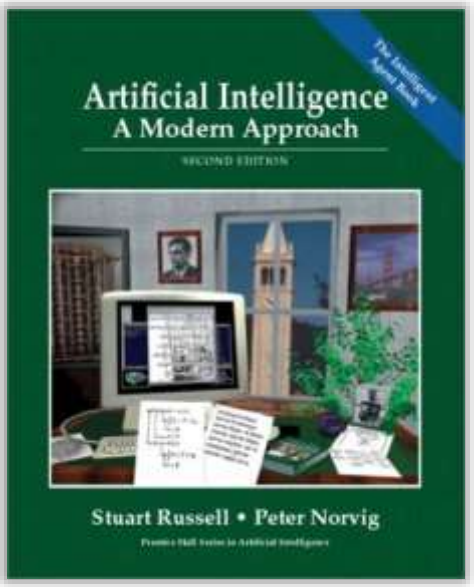
К оглавлению

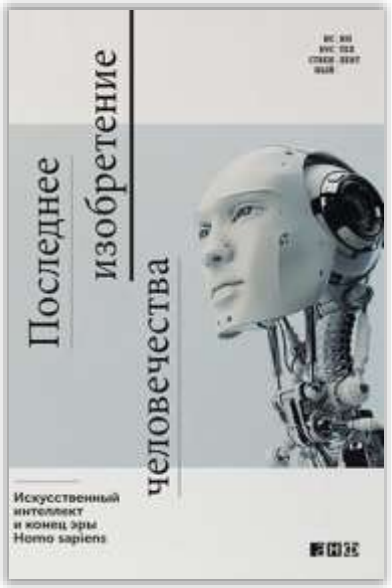
116 7 книг об искусственном интеллекте















117 Определение ИИ

"…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.



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

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)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(1) OJ C 229, 31.7.2012, p. 90.
(2) OJ C 391, 18.12.2012, p. 127.
(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
(4) 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 L 281, 23.11.1995, p. 31).

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:

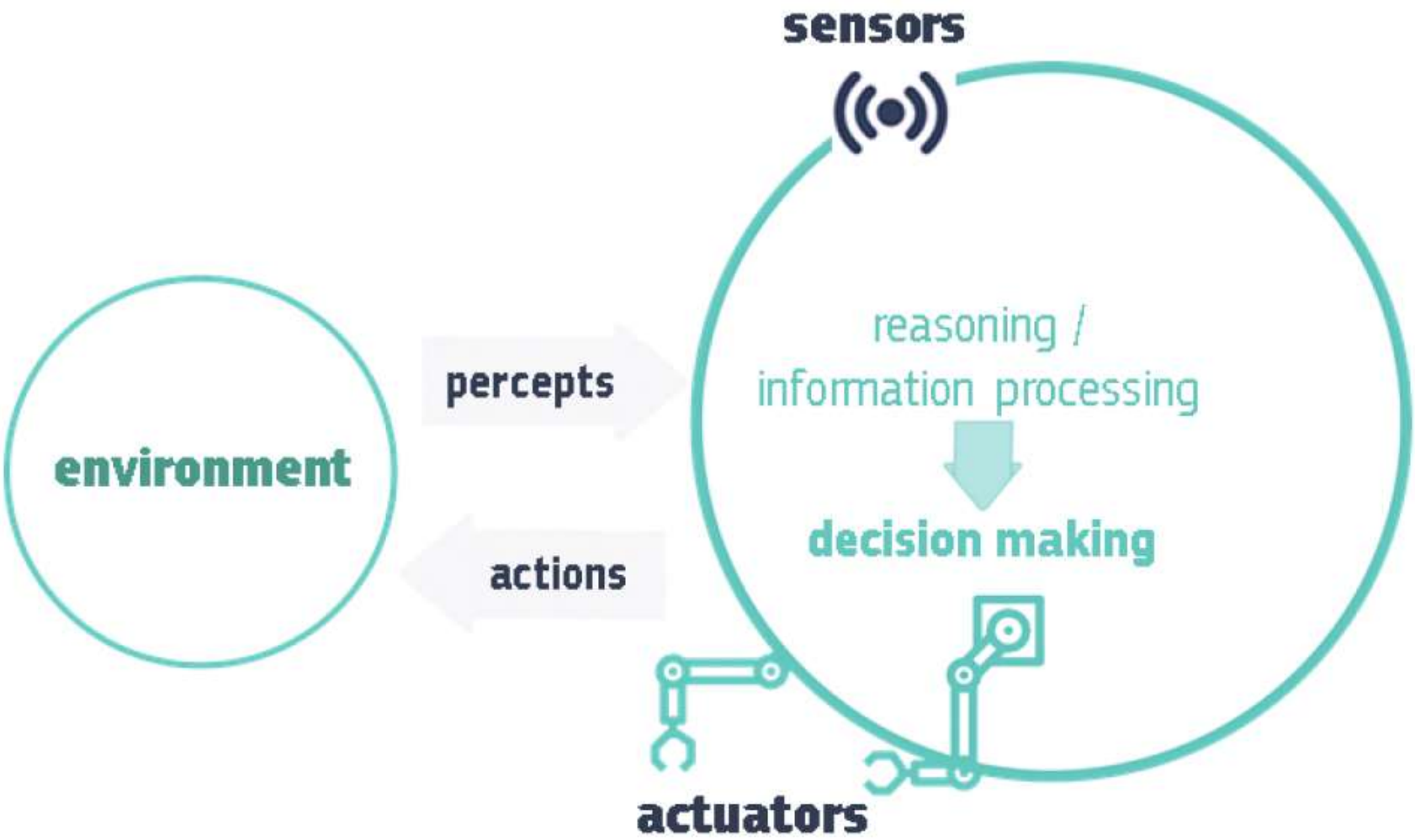
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(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.

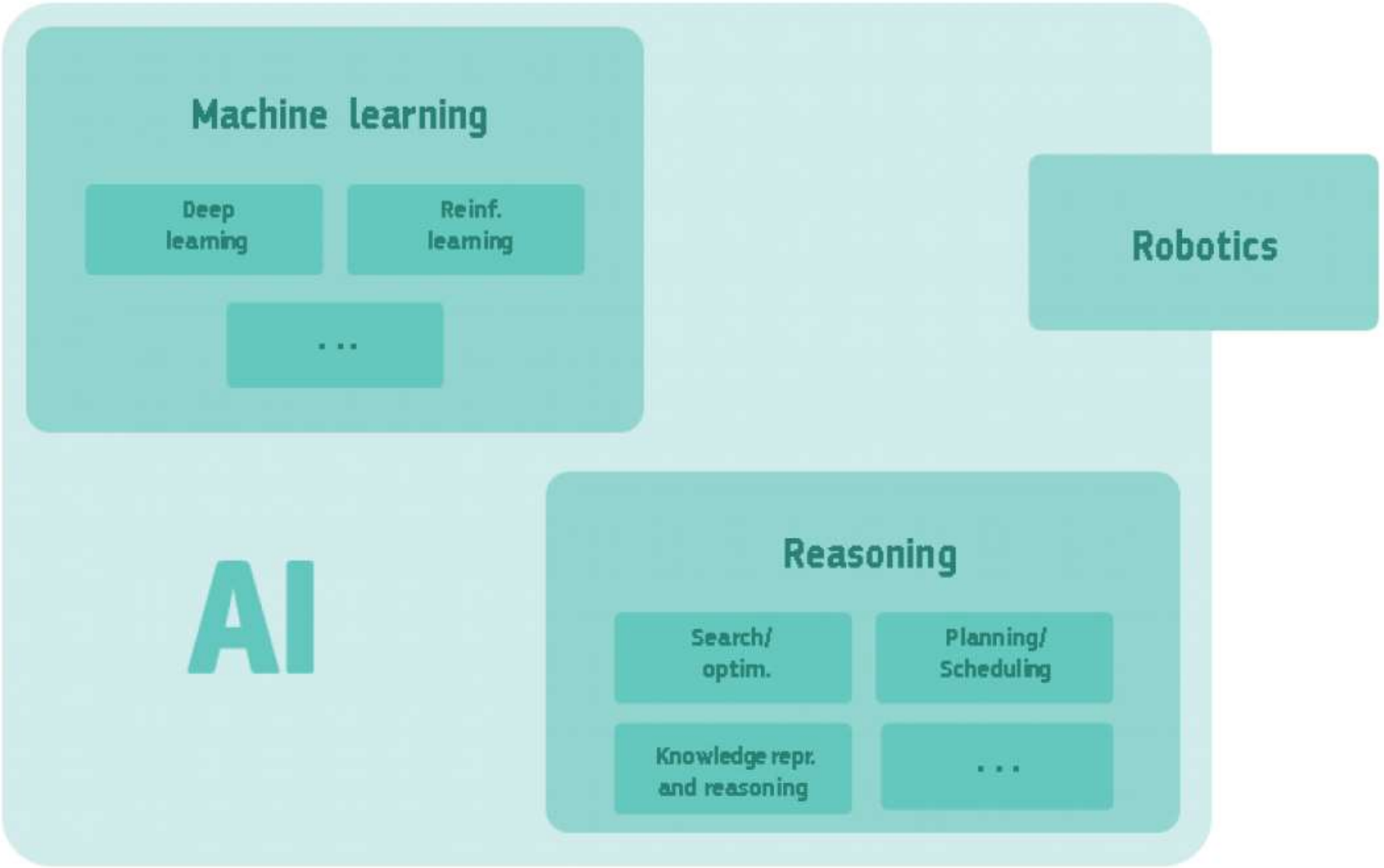
3. In the cases referred to in points (a) and (c) of paragraph 2, **the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests**, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

119 Схематичное определение ИИ-систем



https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

Упрощенная схема соотношения области знаний об ИИ с иными областями



https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

Белая книга по искусственному интеллекту - европейский подход к совершенству и доверию



EUROPEAN
COMMISSION

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 2018[1]. 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 Guidelines[2] 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.

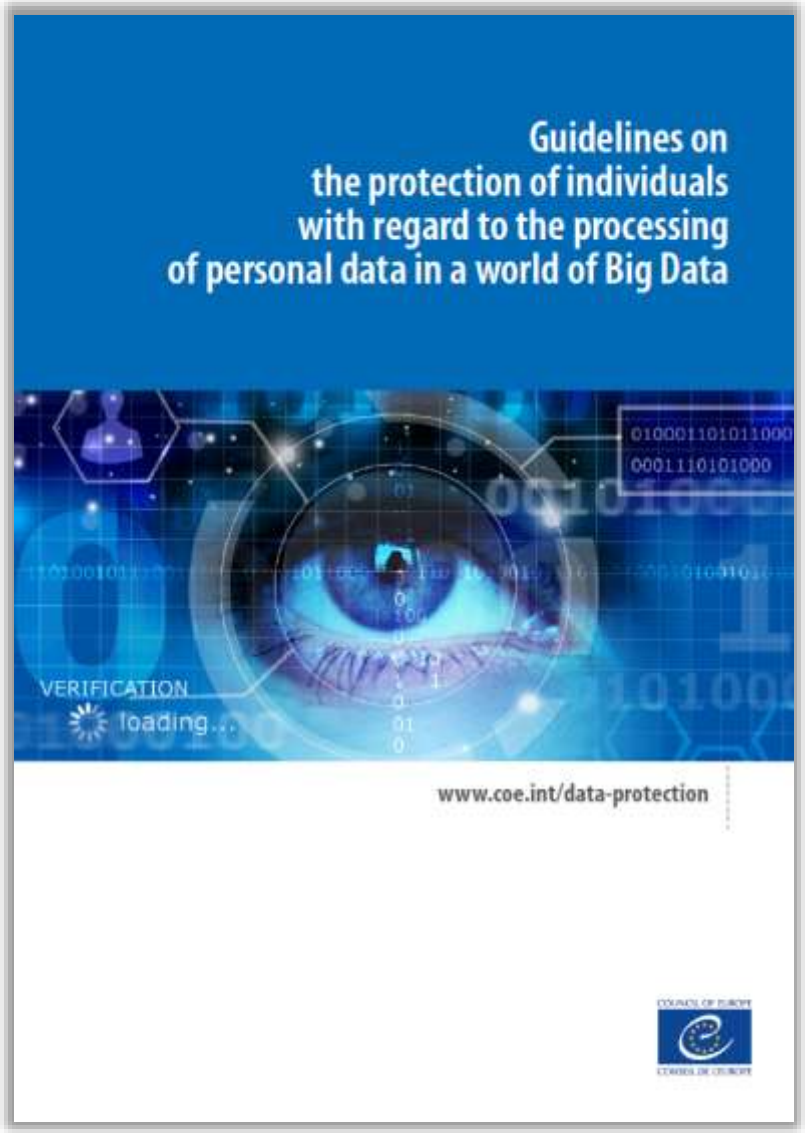
Thus, the Commission supports a regulatory and investment oriented approach with the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of this new technology. The purpose of this White Paper is to set out policy options on how to achieve these objectives. 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.

https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

Руководство от СЕ по защите физических лиц при обработке персональных данных в мире больших данных



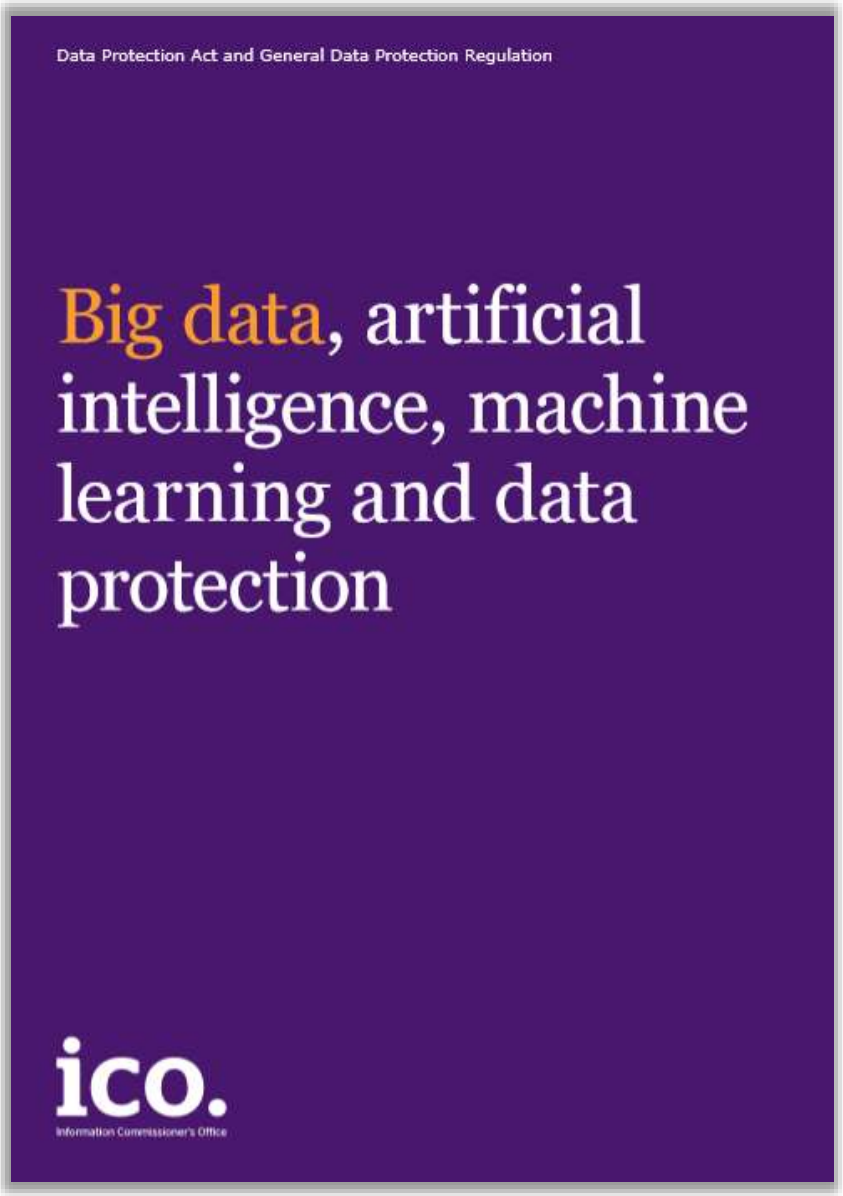
Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data

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.

https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificial-intelligence-and-personal-data-protection
https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0

Исследование ICO о влиянии больших данных, ИИ и машинного обучения

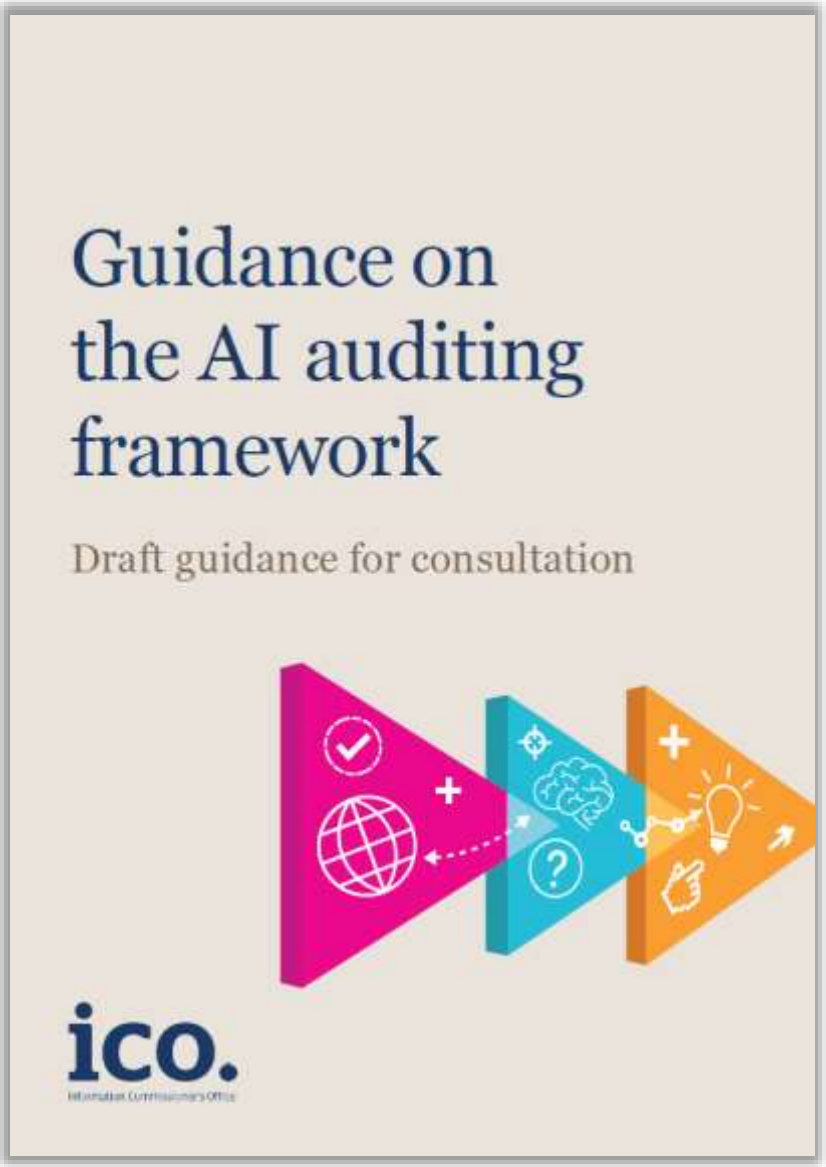


Big data, artificial intelligence, machine learning and data protection

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.

https://ico.org.uk/media/for-organisation/documents/2013559/big-data-ai-ml-and-data-protection.pdf

124 Руководство ICO по основам аудита ИИ



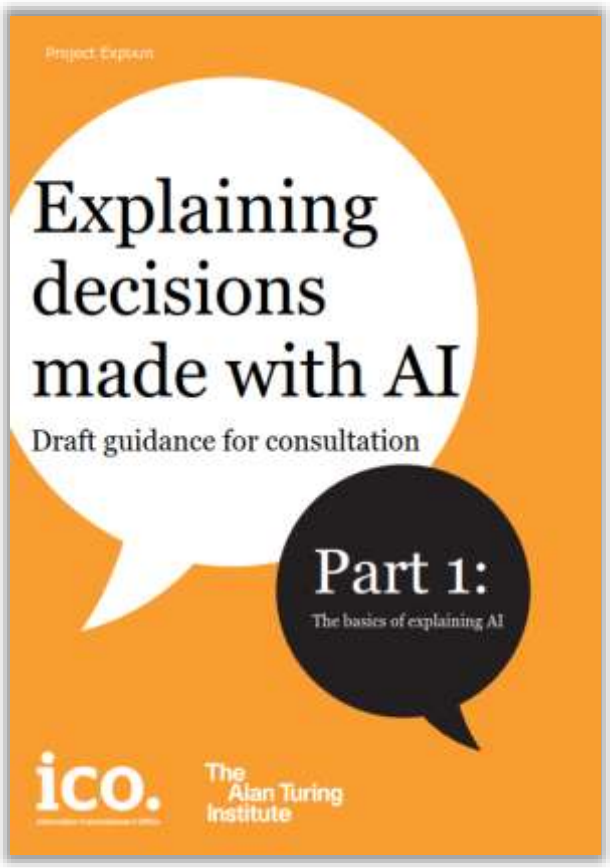
Guidance on the AI auditing framework

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.

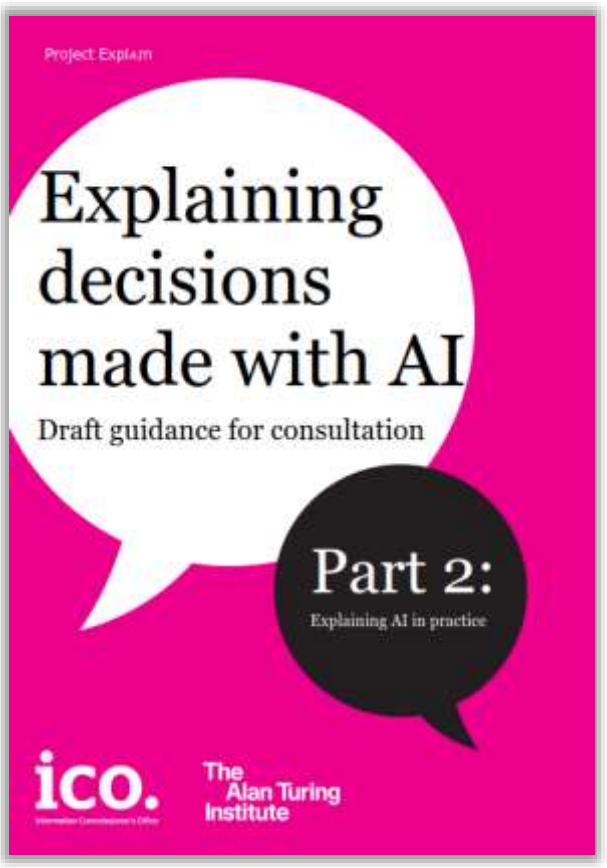
Руководство содержит рекомендации о том, как понимать закон о защите данных в отношении регулирования технологий ИИ, и рекомендации по организационным и техническим мерам по снижению рисков, которые ИИ представляет для отдельных лиц. Документ также предоставляет надежную методологию для аудита систем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

https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-ai-auditing-framework-guidance-for-organisations

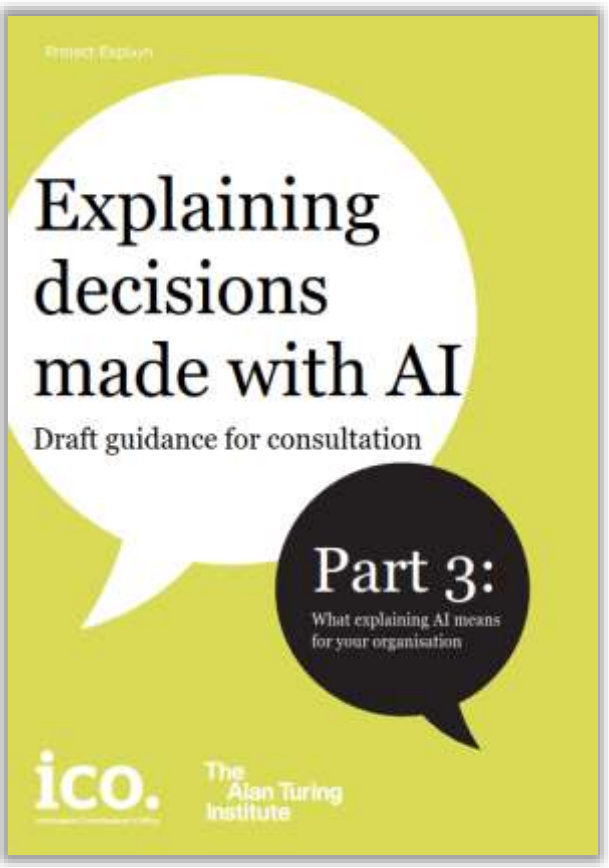
Руководство по разъяснению принимаемых ИИ решений от ICO и Института им. Алана Тьюринга



Part 1: The basics of explaining AI



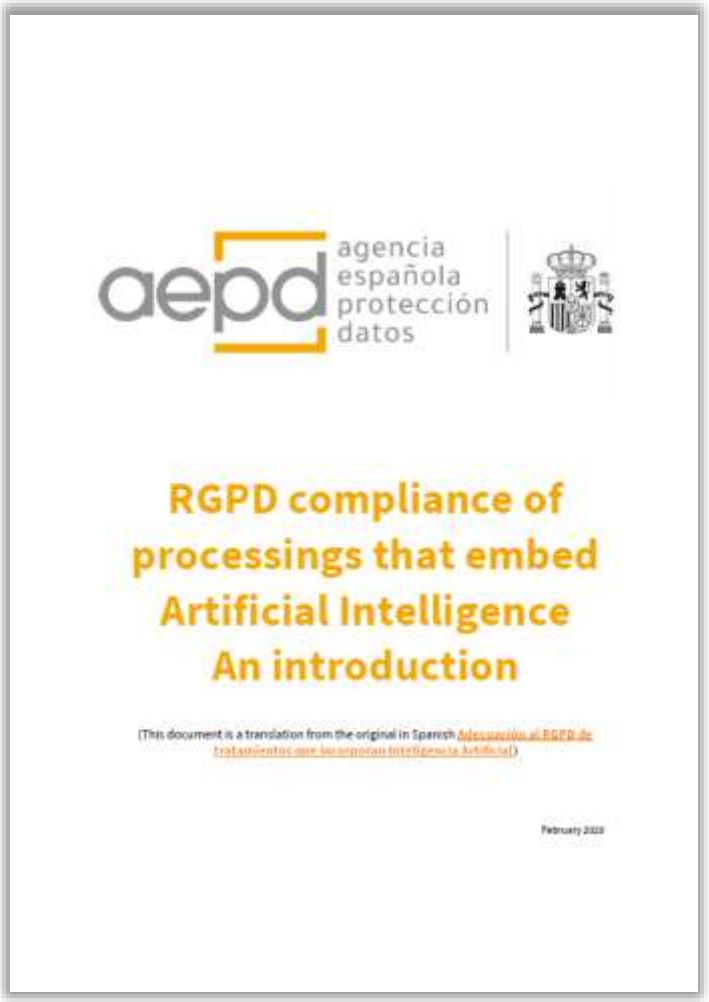
Part 2: Explaining AI in practice



Part 3: What explaining AI means for your organisation

https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-and-the-turing-consultation-on-explaining-ai-decisions-guidance/

Руководство AEPD по использованию технологий ИИ в контексте требований GDPR



I. INTRODUCTION TO THE AI FRAMEWORK AND DATA PROTECTION
A. AI Techniques
B. Data processing by means of AI solutions
C. Data protection and ethical dimension
D. GDPR definitions
E. Life cycle of an AI solution
F. Personal data processing by means of AI
G. Assessment of AI-based solutions
H. Short summary of obligations lay down by the GDPR

II. ROLES, RELATIONSHIPS AND RESPONSABILITIES

III. COMPLIANCE
A. Lawfulness and limited purpose
Legitimate interest
Special categories
Processing for compatible purposes
B. Information
Relevant information on the implemented logic
C. General aspects related to the exercise of rights
D. Right to access
E. Right to erasure
Limitations to erasure
F. Blocking of data
G. Right to rectification
H. Portability
I. Decision-making based on automated processing

IV. PRIVACY RISKS MANAGEMENT
A. Risk assessment
B. Privacy Impact Assessment-(PIA)
C. Transparency
During training
Certification
Automated decisions and profiling
Data controller personnel
The Data Protection Officer as a tool for transparency
D. Accuracy
Factors affecting accuracy
Biometric information
Profiling combination
Verification vs. Validation
Accuracy assessment as continuous process
E. Minimisation
Training data
Minimisation techniques
Extent of the data categories in an AI-based solution
Extent of the training set
Personal data in the AI-based solution
F. Security
Specific threats in AI components
Logs or activity records
G. Assessment of the proportionality and the need for such processing
H. Audit

V. INTERNATIONAL TRANSFERS

VI. CONCLUSIONS

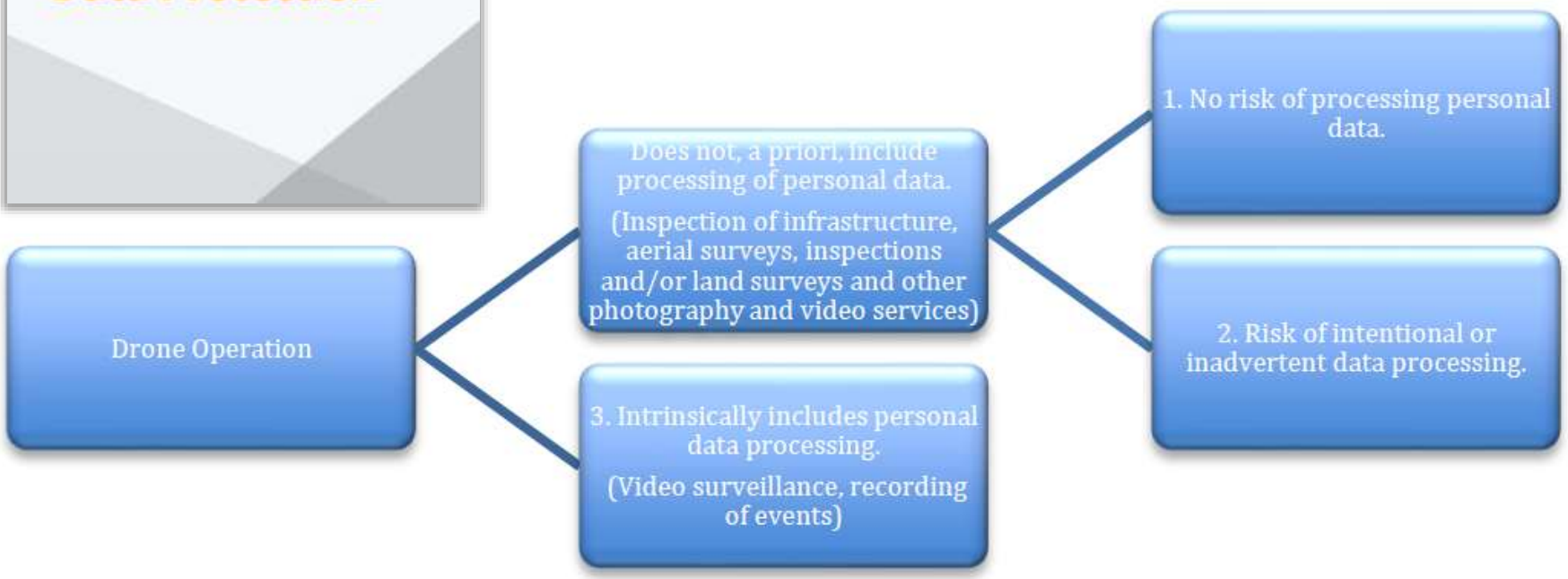
VII. REFERENCES

VIII. ANNEX: CURRENT AI-BASED SERVICES

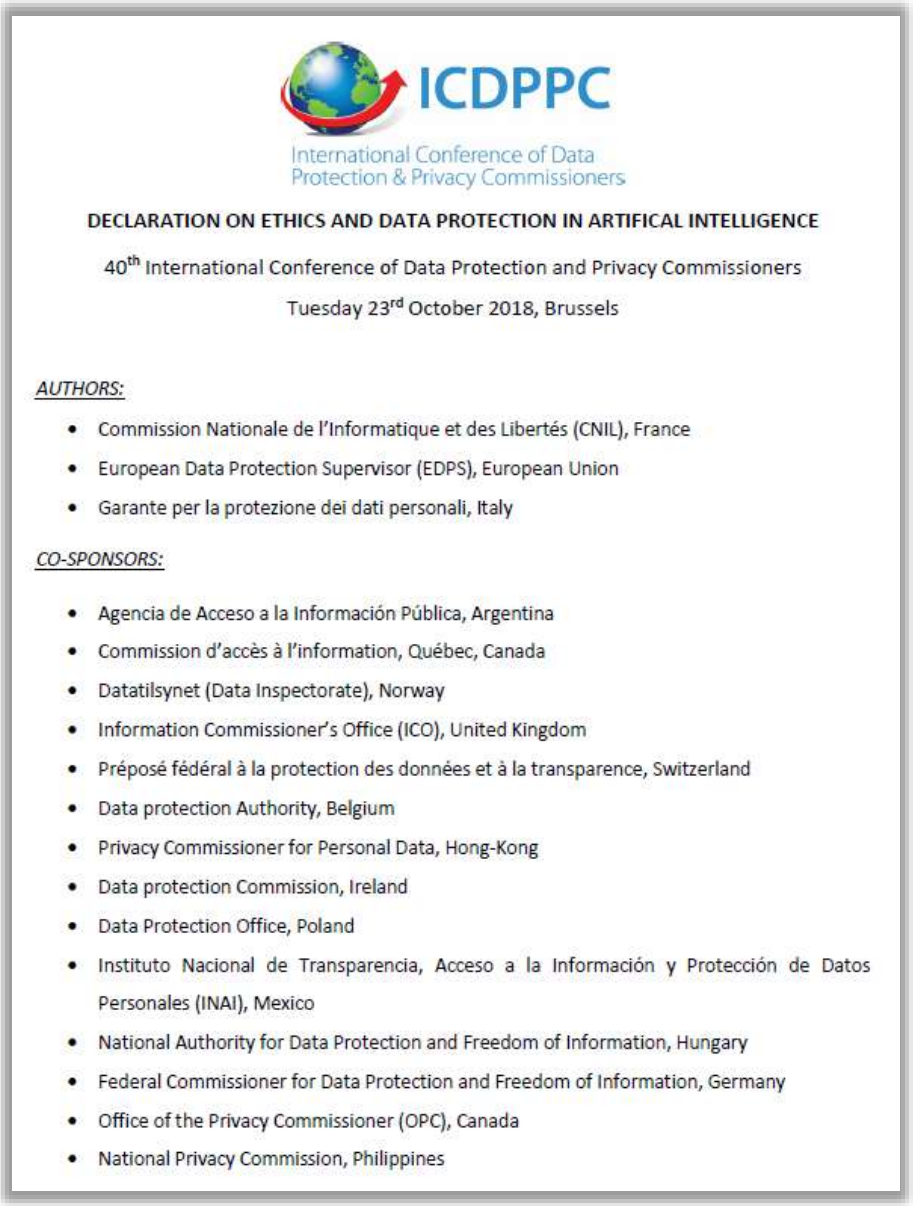
https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia-en_0.pdf

Руководство AEPD по защите персональных данных при использовании дронов





https://www.aepd.es/sites/default/files/2019-12/guia-drones-en.pdf



ICDPPC

International Conference of Data Protection & Privacy Commissioners

DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL 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 artifical 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).

https://www.privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

Отчет от СЕ «Искусственный интеллект и защита данных: вызовы и возможные ответы на них»



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

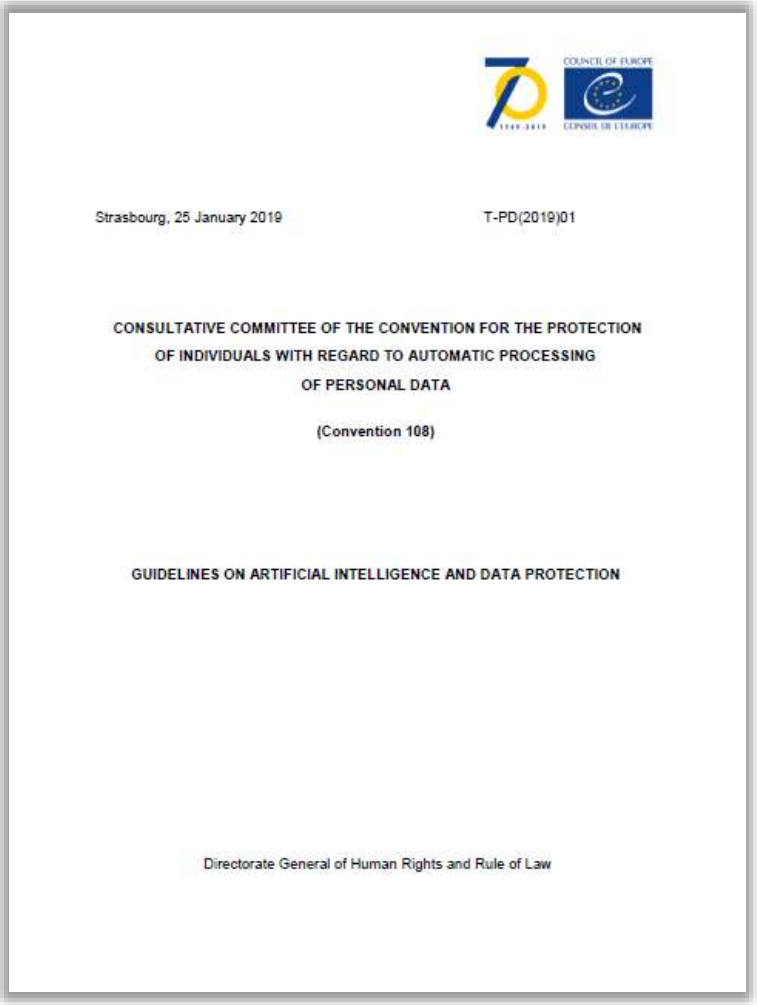
Directorate General of Human Rights and Rule of Law

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.

https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificial-intelligence-and-personal-data-protection
https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

Руководство от СЕ по защите персональных данных при использовании искусственного интеллекта



Strasbourg, 25 January 2019 T-PD(2019)01

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

(Convention 108)

GUIDELINES ON ARTIFICIAL INTELLIGENCE AND DATA PROTECTION

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.

https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificial-intelligence-and-personal-data-protection
https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

Руководство по этике для благонадежного искусственного интеллекта от ЕС



Ethics Guidelines for Trustworthy AI

В апреле 2019 года был 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 предлагают 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.

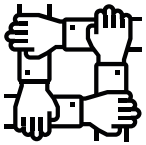
https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

Признаки и качества «благонадежного и человечного» ИИ



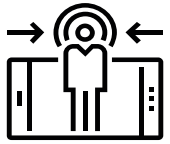
Lawful

Respecting all applicable laws and regulations



Ethical

Respecting ethical principles and values



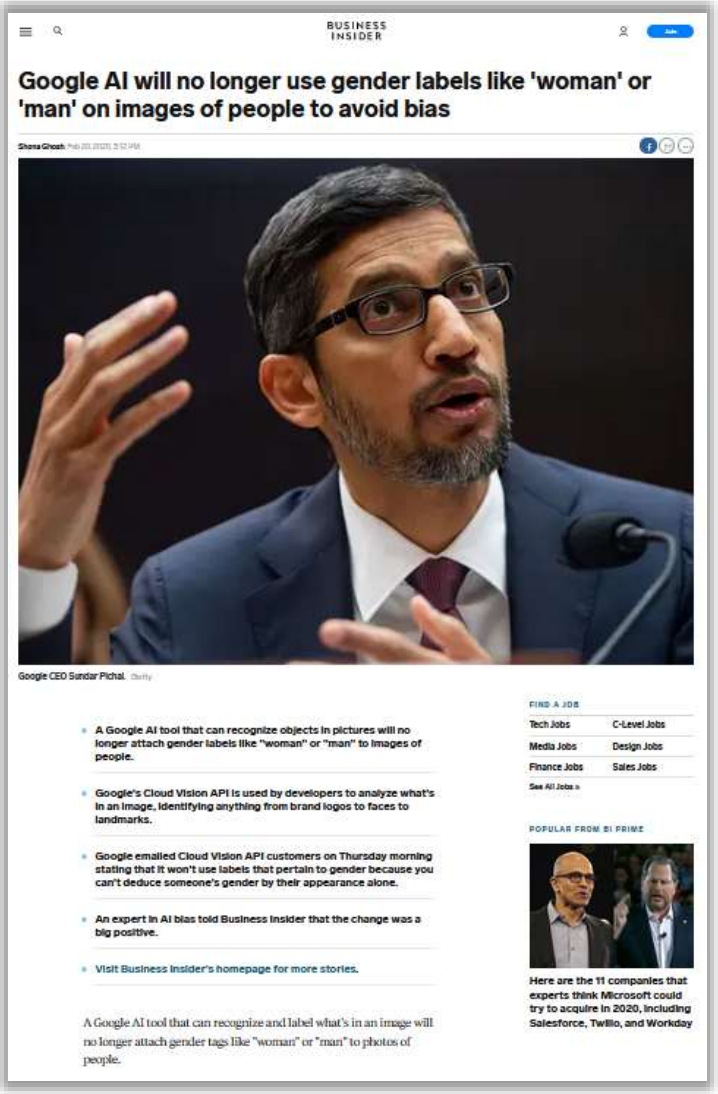
Robust

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

https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

Google Cloud Vision запретили определять пол людей на фото



BUSINESS INSIDER

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

Google CEO Sundar Pichai.

- 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 BI 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.

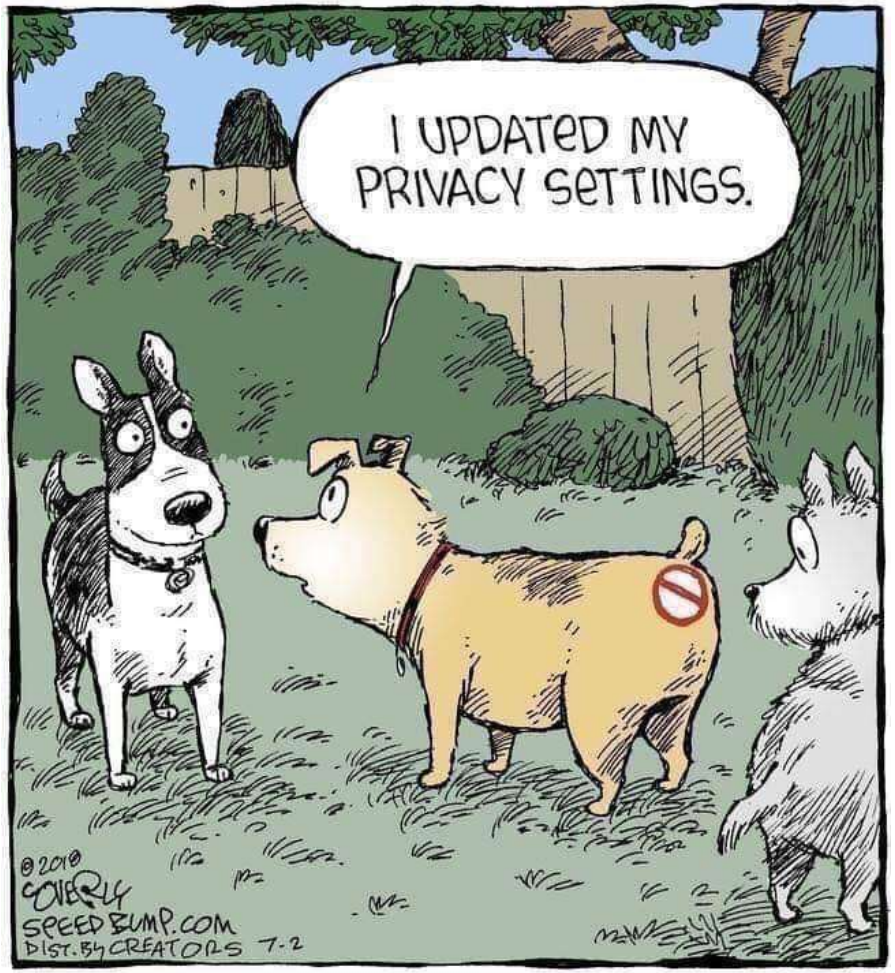
Речь идёт о сервисе Google Cloud Vision API, который, помимо всего прочего, позволяет разработчикам ставить метки на фотографии, идентифицируя изображённые на них объекты. Теперь же алгоритмы не смогут выводить надписи «мужчина» или «женщина» на снимках.

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».

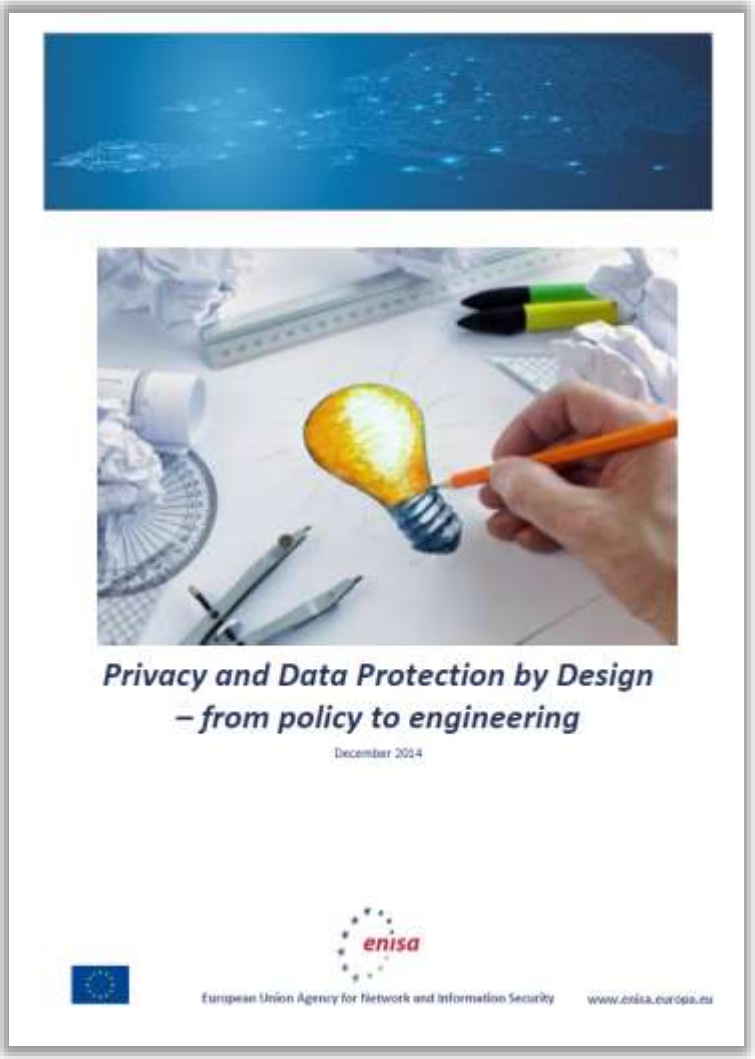
https://www.businessinsider.com/google-cloud-vision-api-wont-tag-images-by-gender-2020-2

Data Protection (Privacy) by Design and by Default



К оглавлению

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



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.

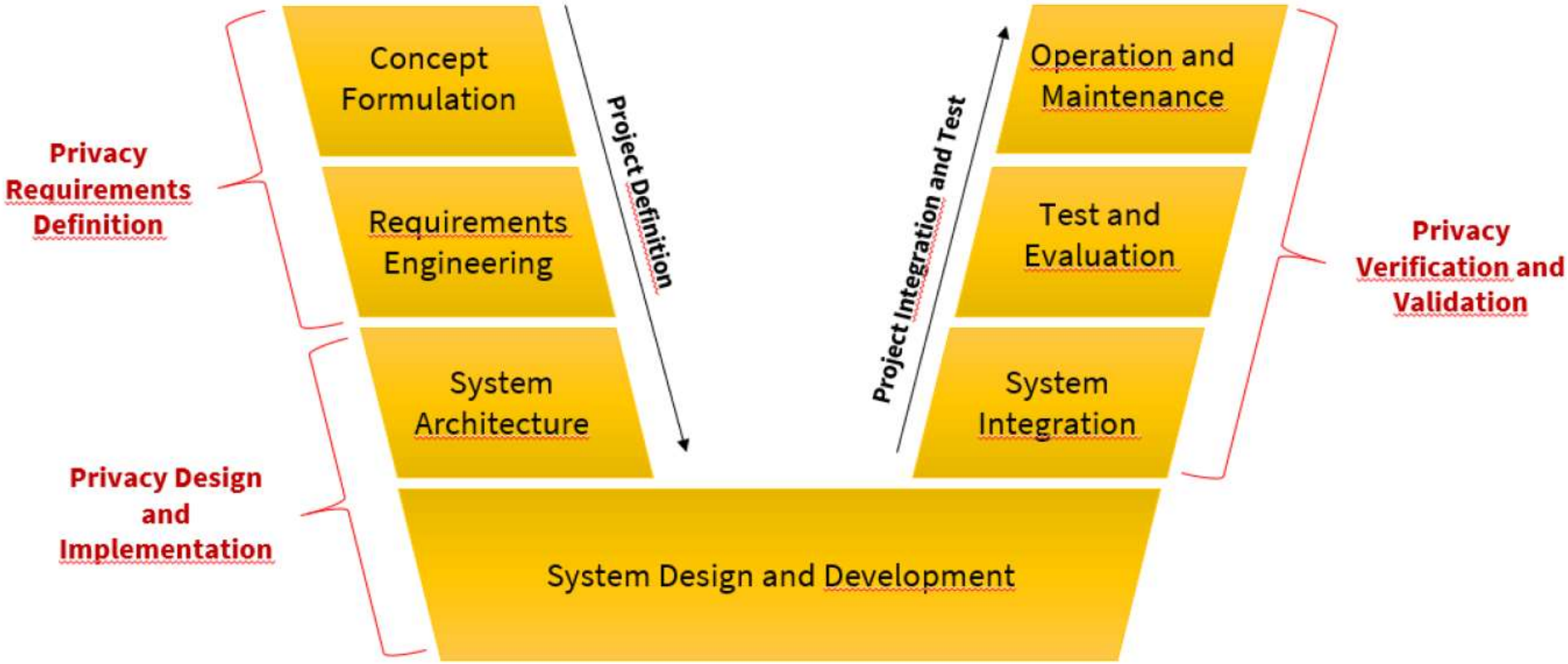
https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

Практическое руководство от AEPD по Privacy by Design: принципы



https://www.aepd.es/media/guias/guia-privacidad-desde-diseno_en.pdf

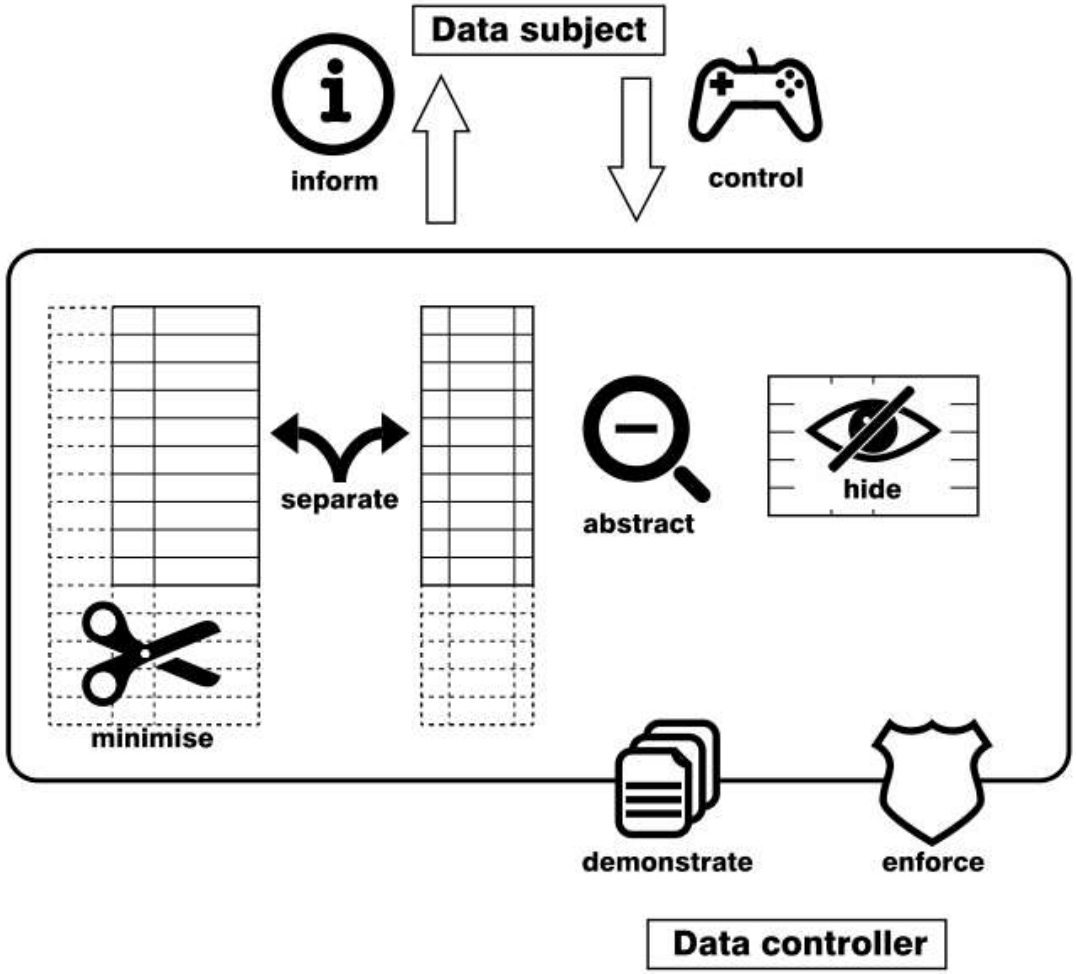
Практическое руководство от AEPD по Privacy by Design: Privacy Engineering



https://www.aepd.es/media/guias/guia-privacidad-desde-diseno_en.pdf

Практическое руководство от норвежского Datatilsynet по Data Protection by Design and by Default при разработке ПО





https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/
https://iapp.my.salesforce.com/sfc/p/#1a000000HSGV/a/1P000000XeRI/BLoR6h6WxzYxtGy7cnVic6new4k9BzwpeFHsPTTpkeg

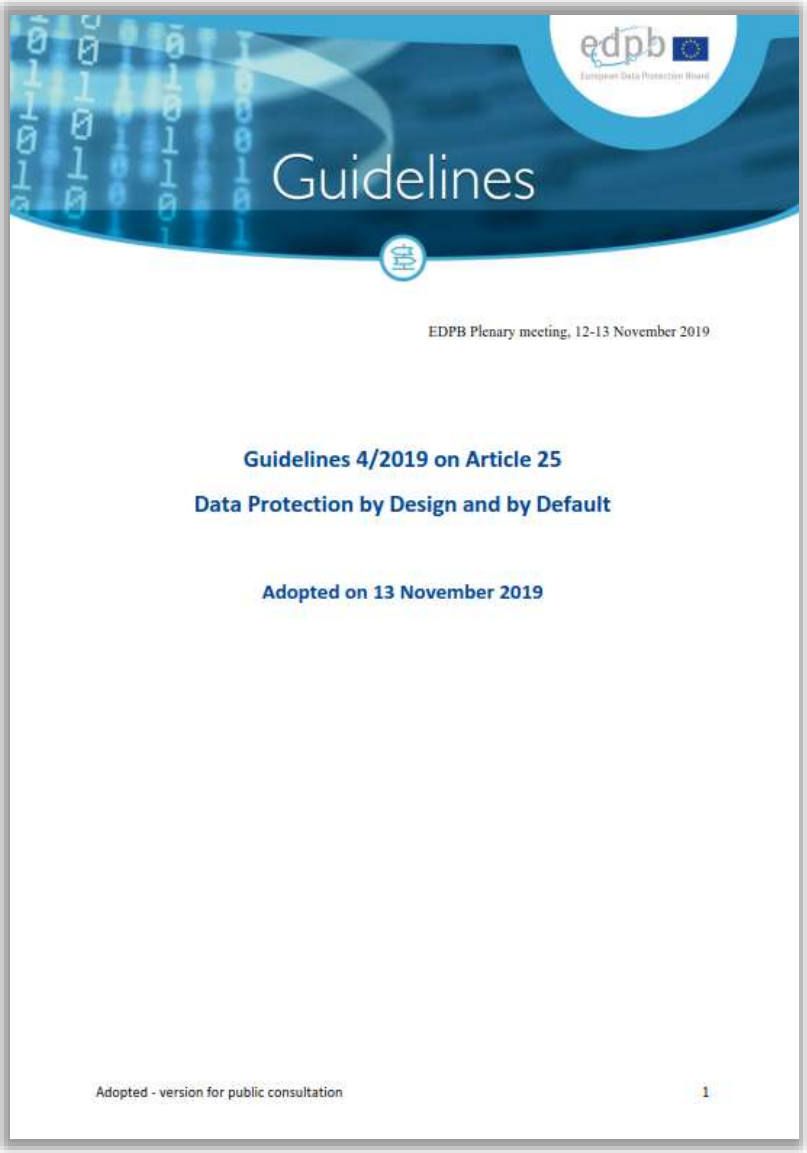
Мнение EDPS от 2018 года о способах реализации принципов Privacy by Design



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

https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en

Руководство EDPB по Data Protection by Design and by Default



Европейский совет по защите данных (European Data Protection Board) опубликовал проект руководства 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.

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

База с паттернами Privacy by Design для разработки ПО

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



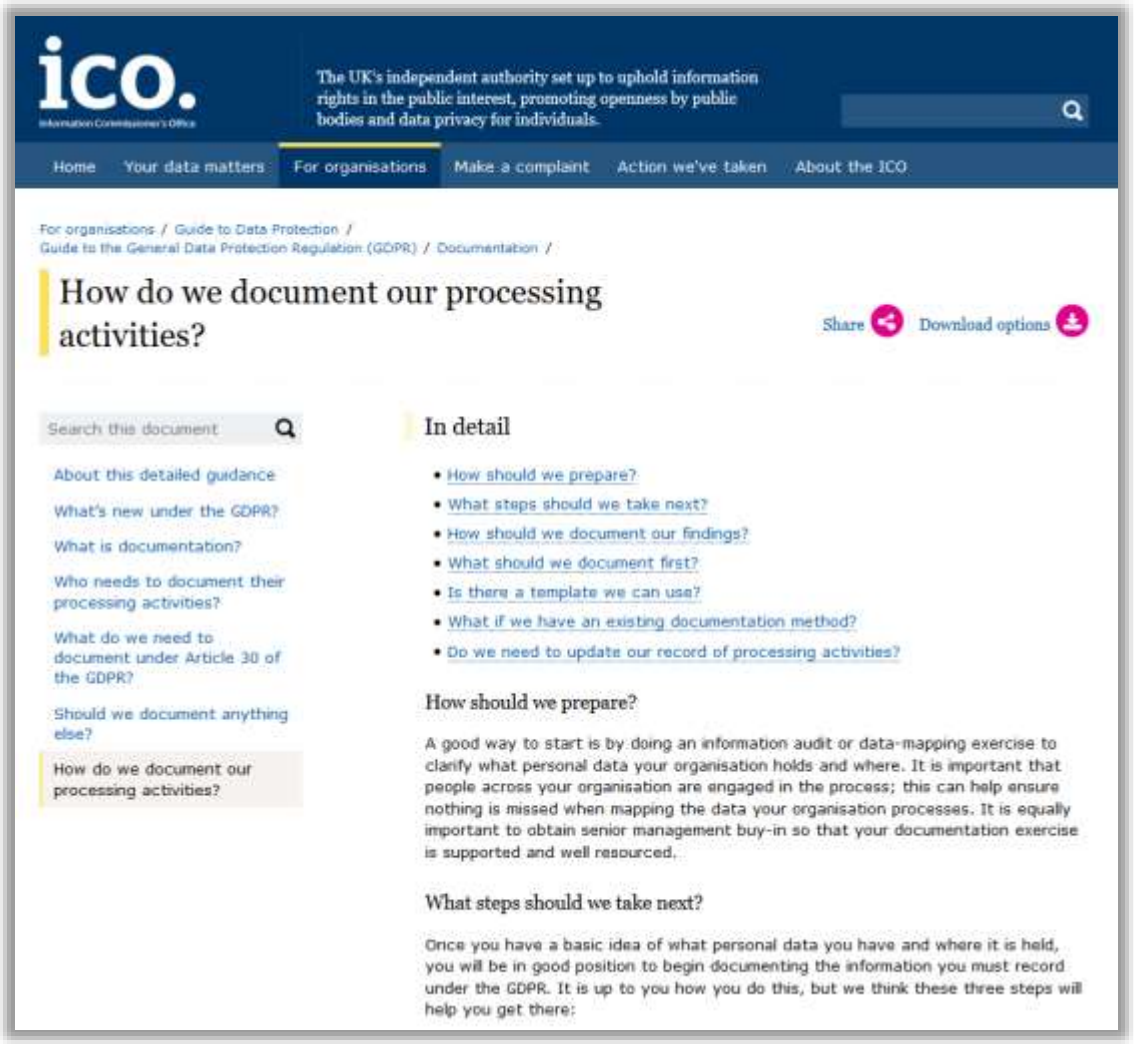
https://privacypatterns.org/

Records of Processing Activities



К оглавлению

Рекомендации по учету процессов обработки данных (RoPA) от ICO



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 контроллеров - 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

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/

Рекомендации по учету процессов обработки данных (RoPA) от GPDP



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

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

VEDI ANCHE: COMUNICATO STAMPA DELL'8 OTTOBRE 2018

RGPD REGOLAMENTO (UE) 2016/679 FAQ

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.

https://www.garanteprivacy.it/en/home/faq/registro-delle-attivita-di-trattamento

Рекомендации по учету процессов обработки данных (ROPA) от CNIL



Description of the processing operation	
Name of the processing operation	
N° / REF	
Date of creation of the processing	
Update of the processing	

Stakeholders	Name	Address	ZIP Code	Town	Country	Phone number	Email address
Controller							
Data protection officer							
DPO's Organisation (if external DPO)							
Representative							
Joint controller(s)							

Purpose(s) of the data processing	
Main purpose	
Sub-purpose 1	
Sub-purpose 2	
Sub-purpose 3	
Sub-purpose 4	
Sub-purpose 5	

Categories 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, GPS data, GSM, etc.)		
Social Security Number (or NIR)		

Special categories 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		

Categories 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.

https://www.cnil.fr/en/record-processing-activities

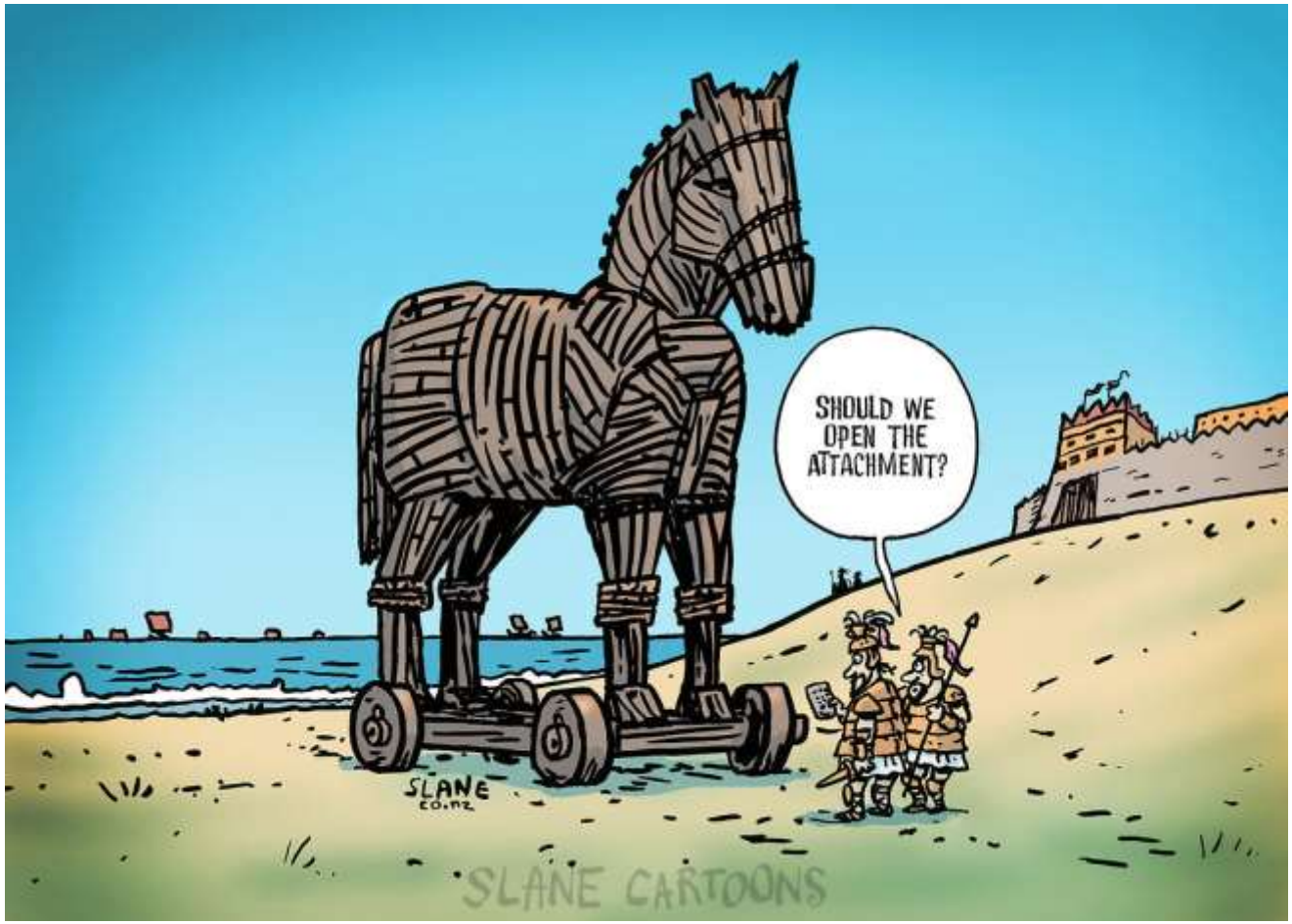
Рекомендации по учету процессов обработки данных (RoPA) для компаний РФ от автора презентации

1.	**Обозначение и наименование процесса**			
1.1.	*Общее описание процесса*			
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.	*Характеристики обработки ПДн*			
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.	Источник[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.	*Взаимодействие с третьими лицами при обработке ПДн*			
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.	Поручение или совместная обработка ПДн	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.

http://sps-ib.ru/ropa.docx

Защита персональных данных



К оглавлению

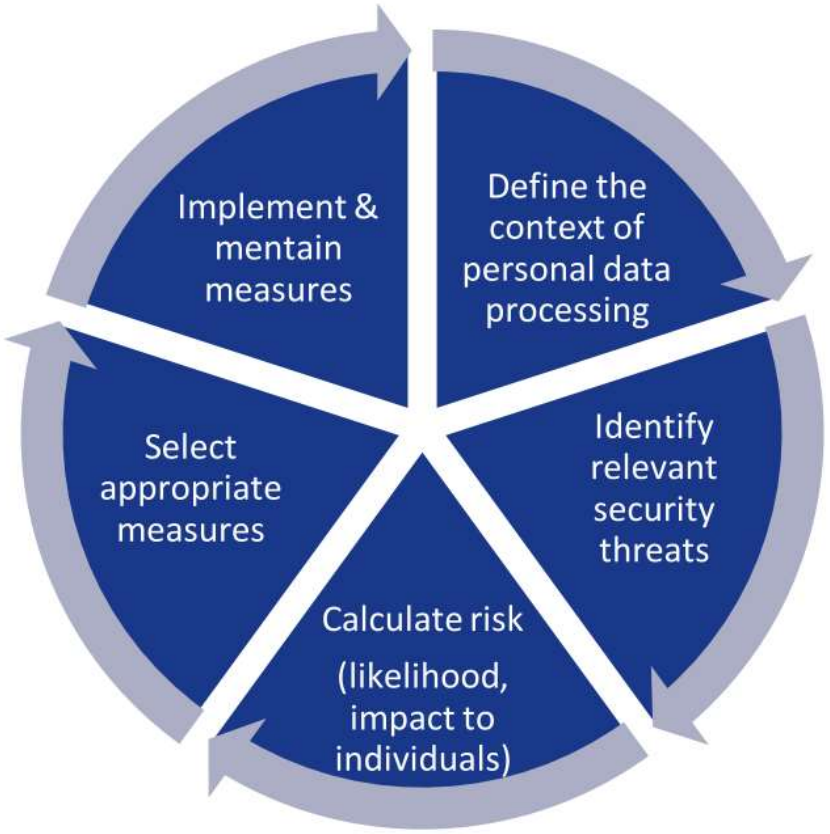
148 Технические и организационные меры защиты в GDPR

Reference	Properties	Category
Recital 29	Pseudonymisation, unlinkability, authorization	PP
Recital 66	Distribute data subject requests to processors	DSR
Recital 67	Restriction of processing	DSR
Recital 68	Data portability request	DSR
Recital 71	Accuracy of data	PP
Recital 78	Data minimization, pseudonymization, information	PP
Recital 81	Security	General
Recital 88	Protect data	General
Recital 156	Data minimization	PP
Art. 4 (5)	Pseudonymity	PP
Art. 5 (1) e	Non-identifiability	PP
Art. 5 (1) e	Storage limitation	PP
Art. 5 (1) f	Integrity and confidentiality	PP
Art. 17 (2)	Distribute data subject requests to processors	DSR
Art. 24 (1)	Demonstrate compliance	PP
Art. 24 (2)	Purpose limitation	PP
Art. 25 (1)	Pseudonymisation	PP
Art. 25 (2)	Data minimization	PP
Art. 28 (1)	meet the requirements of this regulation	General
Art. 28 (3) e	Distribute and execute data subject requests	DSR
Art. 28 (4)	meet the requirements of this regulation	General
Art. 32 (1) a	Pseudonymization	PP
Art. 32 (1) a	Encryption	PP
Art. 32 (1) b	Confidentiality, integrity, availability, resilience	PP
Art. 32 (1) c	access	PP
Art. 34 (3) a	render data unintelligible – (encryption, unlinkability)	PP
Art. 83 (2) d	Technical measures will be taken into account when determining fines	General

https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1052&context=amcis2019

Методологическое руководство от 2016 года для среднего и малого бизнеса по защите данных от ENISA

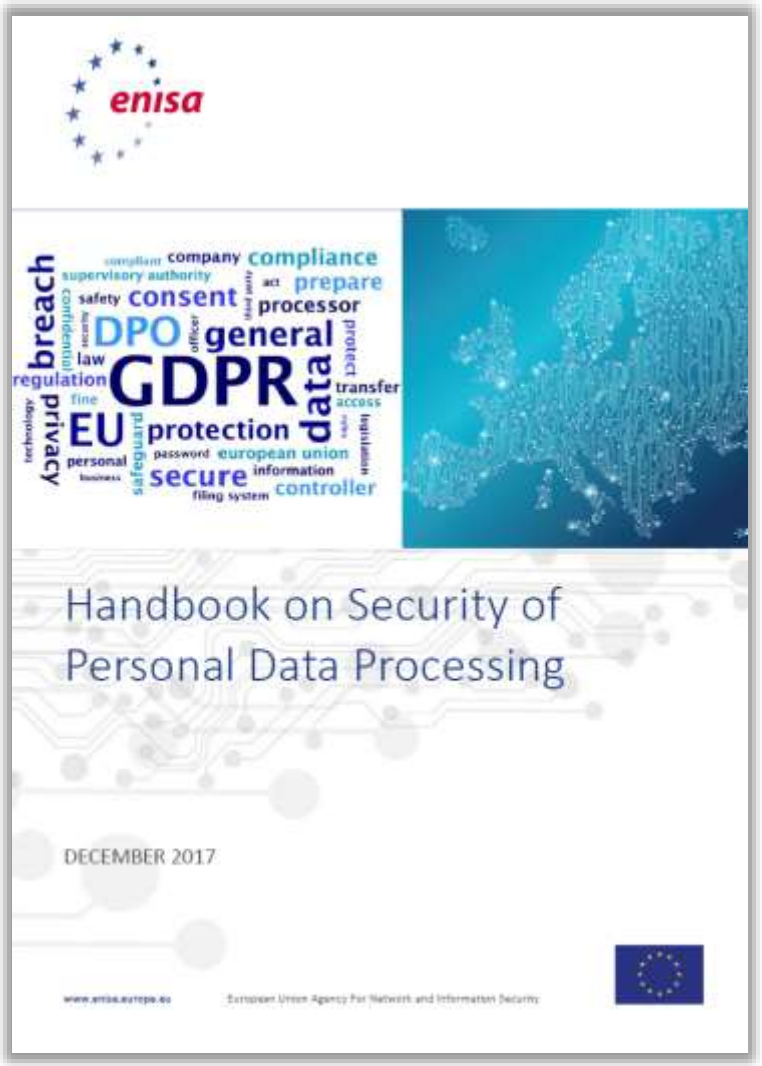




Security risk management for personal data

https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Практическое руководство от 2017 года для среднего и малого бизнеса по защите данных от ENISA



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

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

IMPACT LEVEL

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

Legend

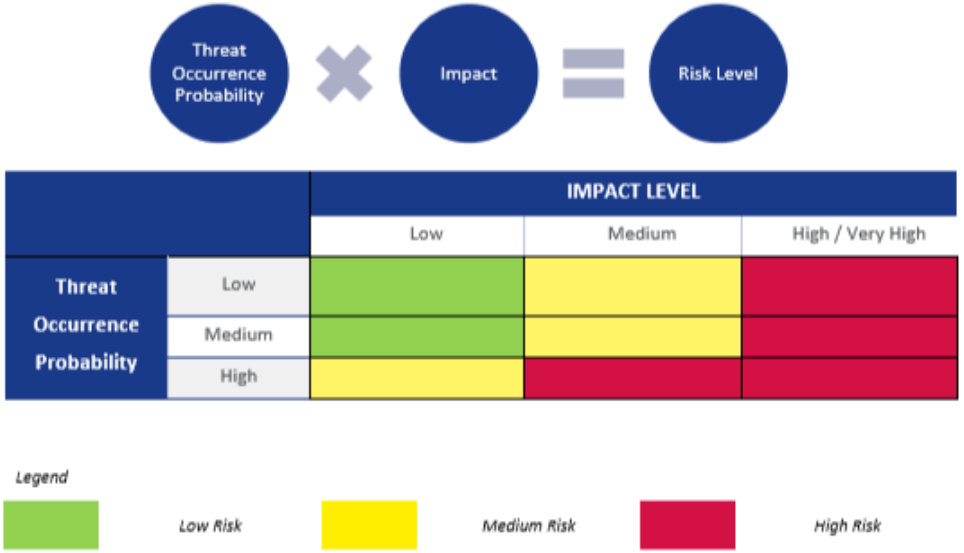
Low Risk | Medium Risk | High Risk

https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Исследование по информационной безопасности в сфере электронных коммуникаций и онлайн-услуг от ENISA



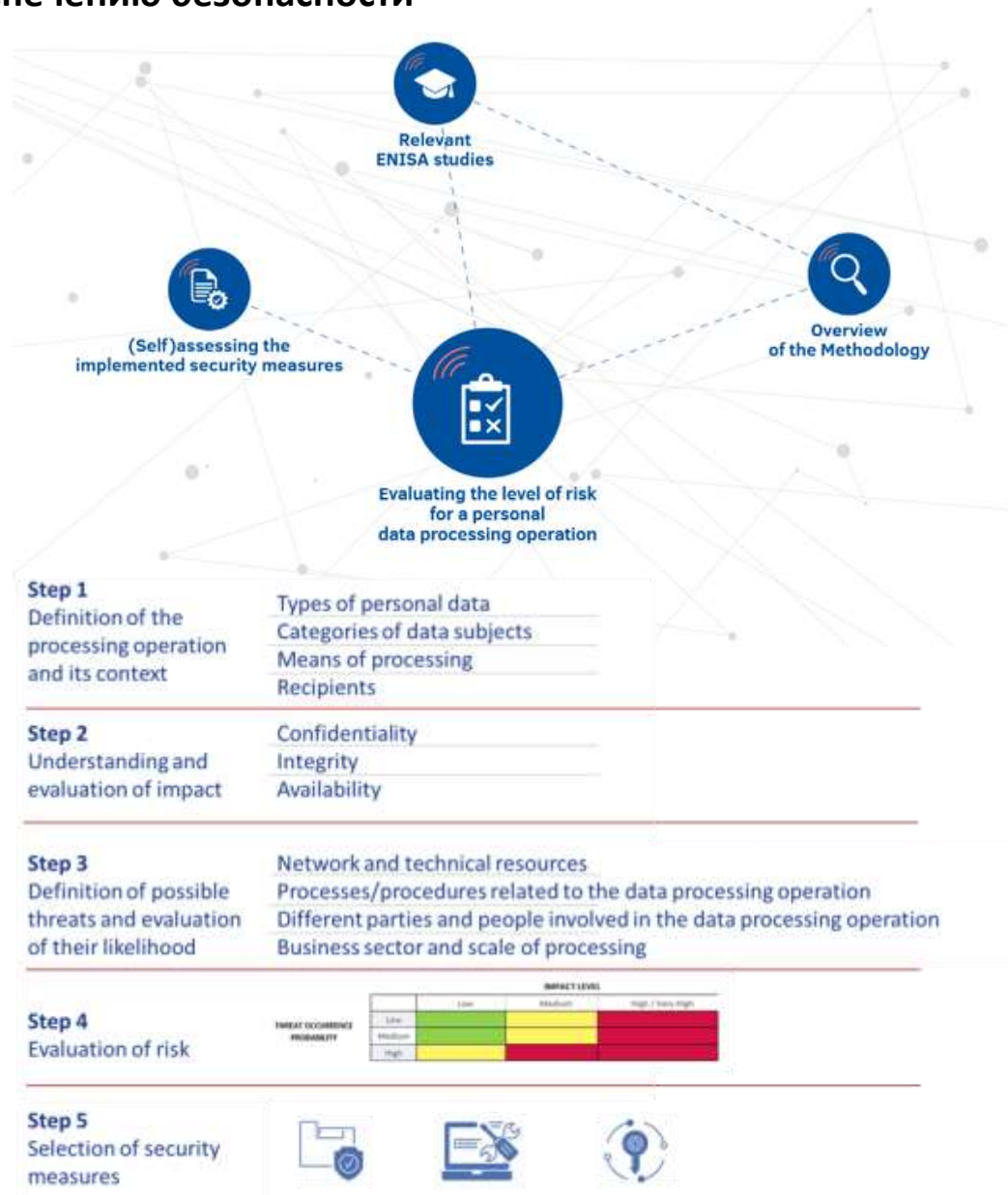
В этом исследовании представлен обзор устоявшихся методов обеспечения информационной безопасности, которой призван помочь среднему и малому бизнесу составить представление о современном уровне развития технологий (State-of-the-Art) защиты информации по ряду направлений, представленных в практическом руководстве ENISA по защите данных.



https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services

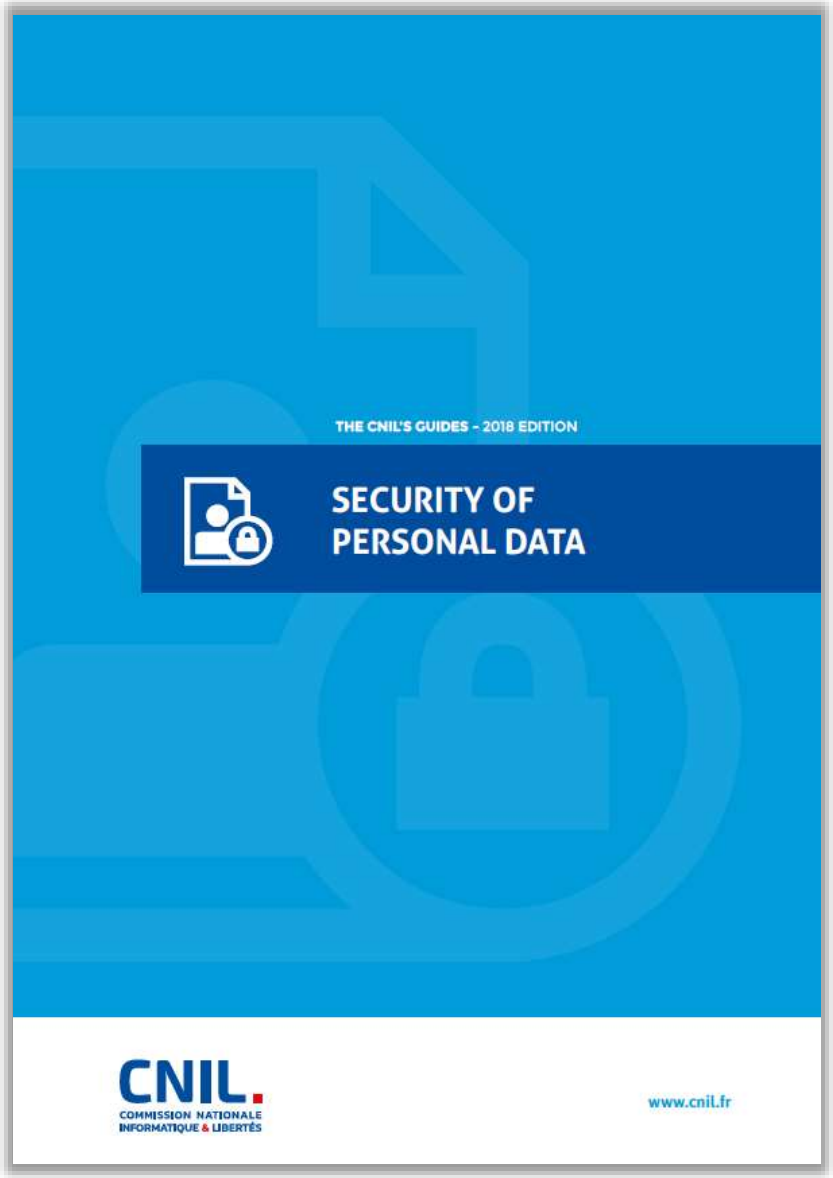
Онлайн-платформа от ENISA по обеспечению безопасности персональных данных





https://www.enisa.europa.eu/risk-level-tool/
https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform

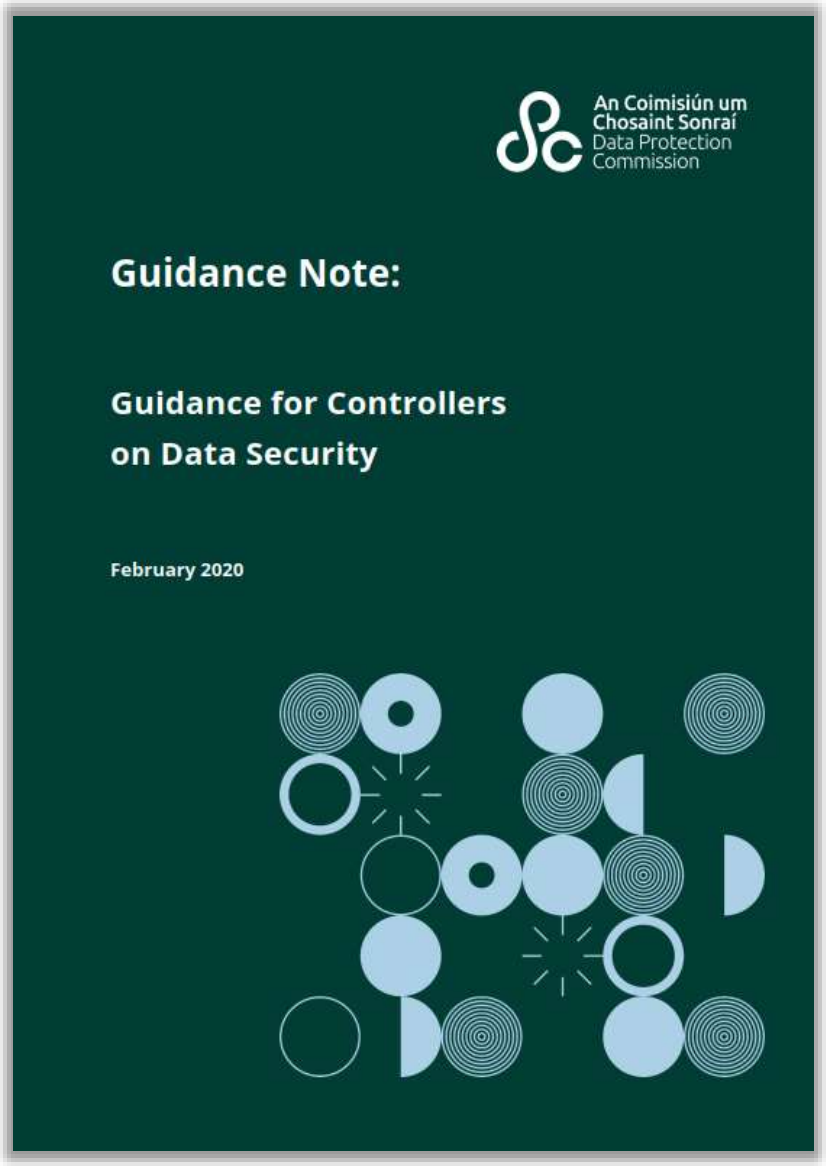
Руководство CNIL от 2018 года по управлению рисками ИБ в рамках обеспечения защиты персональных данных



	FACTSHEET	MEASURE
1	Raising user awareness	Inform and raise awareness among individuals handling data
		Write an IT charter and enforce its application
2	Authenticating	Define a unique identifier (login) for each user
		Adopt a user password policy conform to our recommendations
		Require each user to change his or her password whenever it has been resetted
		Limit the number of access attempts to an account
3	Access Management	Define authorisation profiles
		Remove obsolete access permissions
		Carry out an annual review of authorisations
4	Logging access and managing incidents	Implement a logging system
		Inform users of the implementation of the logging system
		Protect logging equipment and the information logged
		Organise the procedures for personal data breach notifications
5	Securing workstations	Organise an automatic session locking procedure
		Use regularly updated antivirus software
		Install firewall software
		Collect the user's consent before any intervention on his or her workstation
6	Securing mobile data processing	Organise encryption measures for mobile equipment
		Undertake regular data backups and synchronisations
		Require a confidential piece of information to unlock smartphones
7	Protecting the internal network	Limit the network traffic to the bare essentials
		Secure remote access to mobile computing devices via VPN
		Implement the WPA2 or WPA2-PSK protocol for Wi-Fi networks
8	Securing servers	Allow access to tools and administration interface only to qualified individuals
		Install critical updates without delay
		Ensure availability of data
9	Securing websites	Use the TLS protocol and check its implementation
		Check that no password or identifier are transferred via URLs
		Check that the user inputs correspond to what is expected
		Place a consent banner for cookies not required by the service
10	Ensuring continuity	Carry out regular backups
		Store the backup media in a secure place
		Organise security measures for the transport of backups
		Organise and regularly test the business continuity
11	Archiving securely	Implement specific access methods to archived data
		Destroy obsolete archives securely
12	Supervising maintenance and data destruction	Record maintenance in a register
		Have a responsible person from the organisation supervise work by third parties
		Delete the data from all hardware before it is discarded
13	Managing dataprocessors	Add a specific clause in the contracts of subcontractors
		Organise the restitution and destruction conditions of data
		Ensure the effectiveness of provided guarantees (security audits, visits, etc.)
14	Securing exchanges with other organisations	Encrypt data before sending it
		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
16	Supervising software development	Offer parameters that respect the privacy of end users
		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

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf

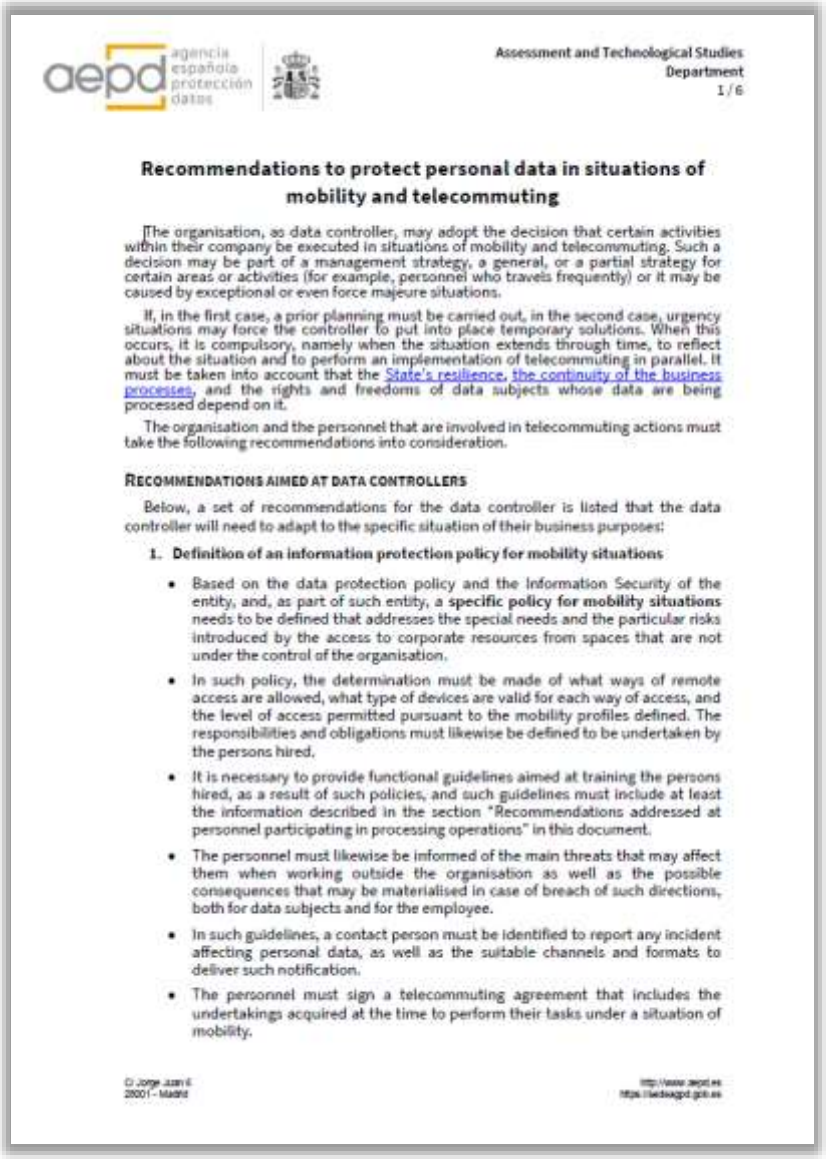
154 Руководство DPC по защите персональных данных



Data Collection and Retention Policies
Access Controls
Access Authentication
Automatic Screen Savers
Encryption
Anti-Virus Software
Firewalls
Software Patching
Remote Access
Wireless Networks
Portable Devices
Logs and Audit Trails
Back-Up Systems
Incident Response Plans
Disposal of Equipment
Physical Security
The Human Factor
Certification

https://www.dataprotection.ie/en/guidance-landing/guidance-controllers-data-security

Рекомендации AEPD по защите персональных данных в условиях мобильности и удаленного взаимодействия



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**

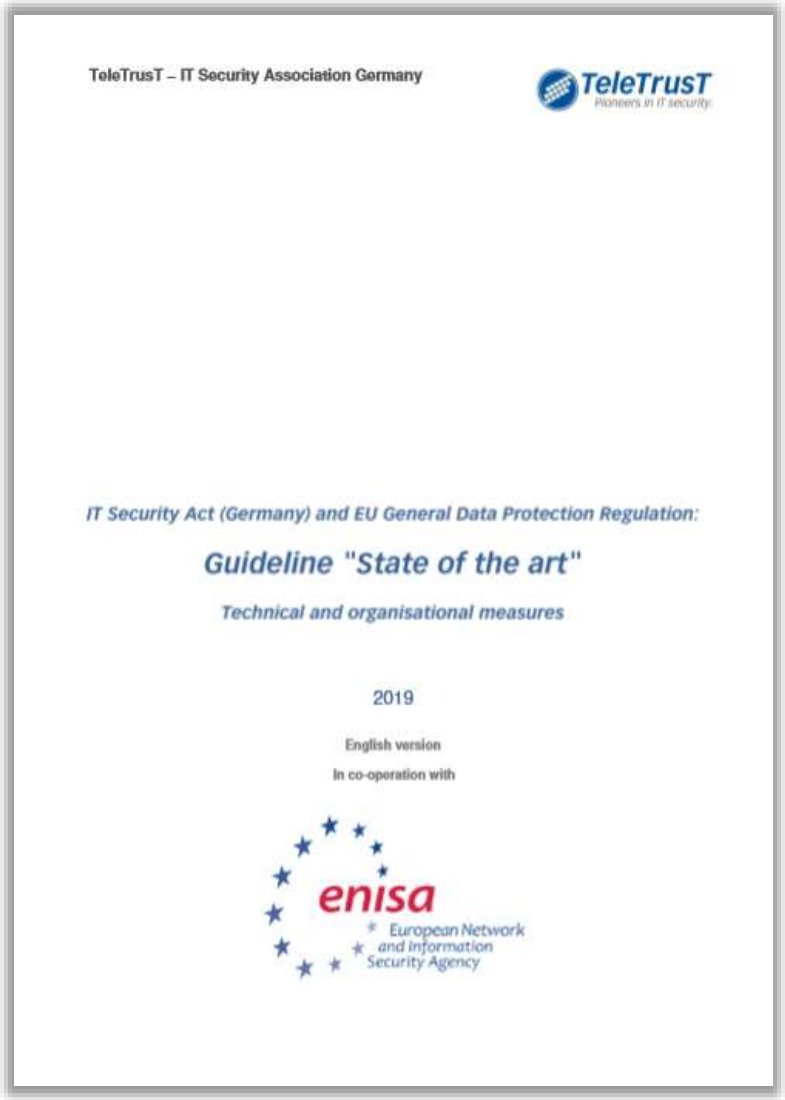
- Based on the data protection policy and the Information Security of the entity, and, as part of such entity, a **specific policy for mobility situations** needs to be defined that addresses the special needs and the particular risks introduced by the access to corporate resources from spaces that are 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.

В апреле 2020 испанский уполномоченный орган опубликовал рекомендации для контроллеров 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.

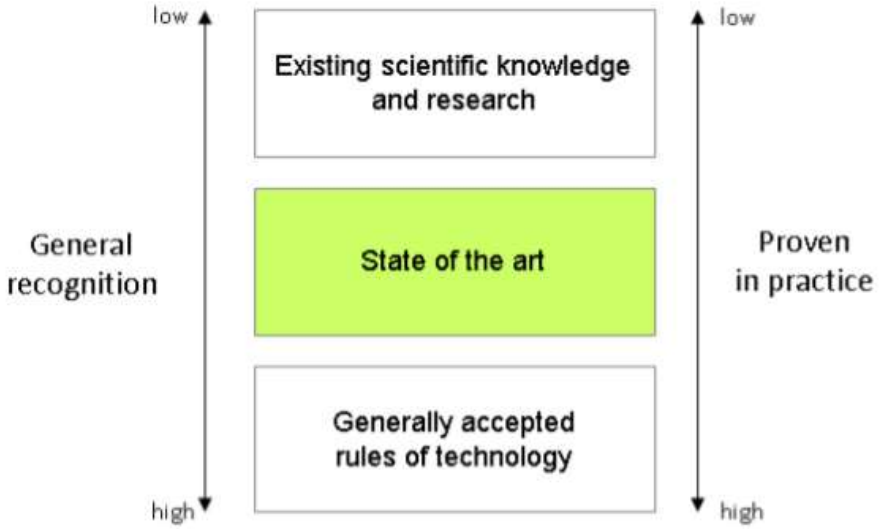
https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteger-datos-teletrabajo-en.pdf

Руководство по современному уровню защиты данных от TeleTrusT



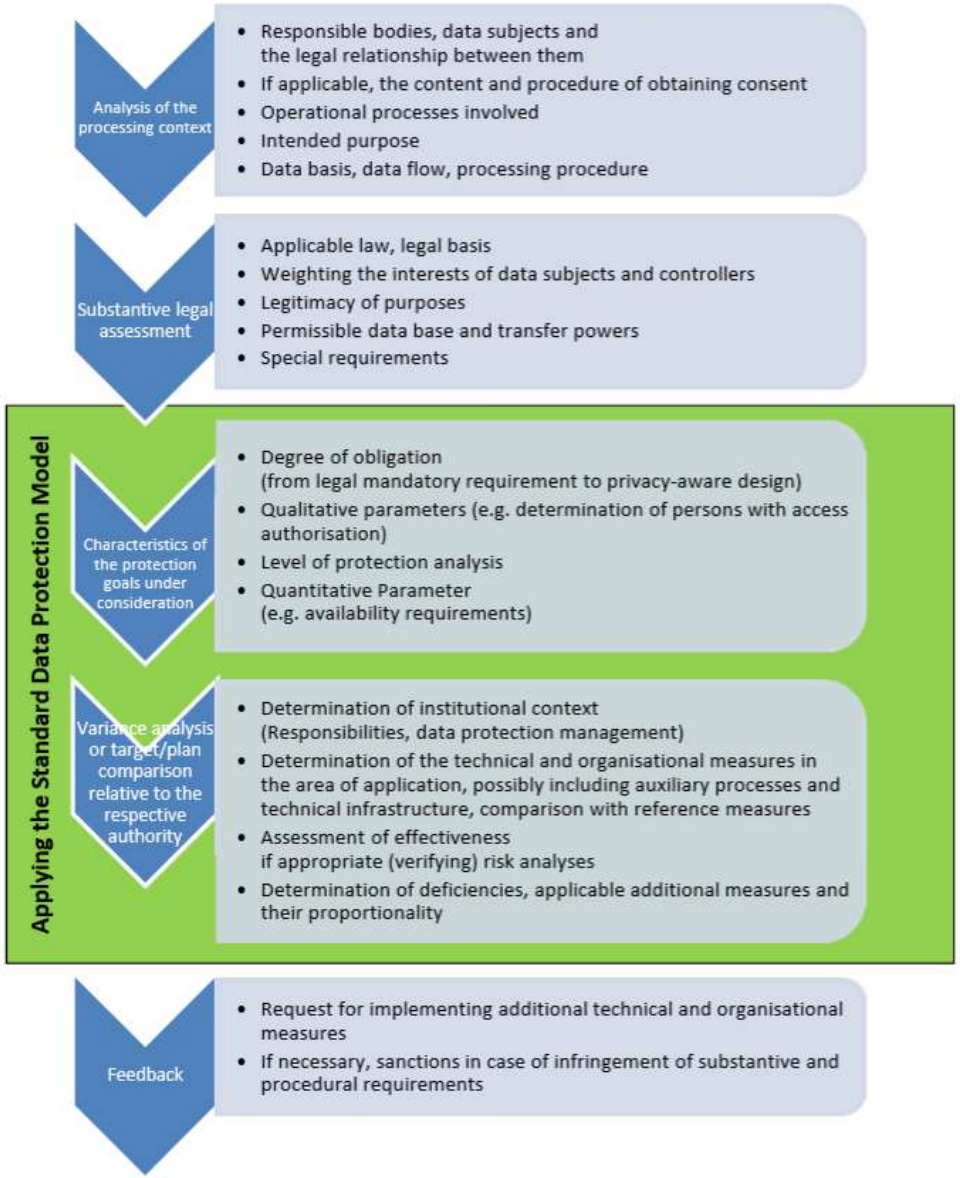
Bundesverband IT-Sicherheit e.V. (TeleTrusT)

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.



https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-02_TeleTrusT_Guideline_State_of_the_art_in_IT_security_ENG.pdf

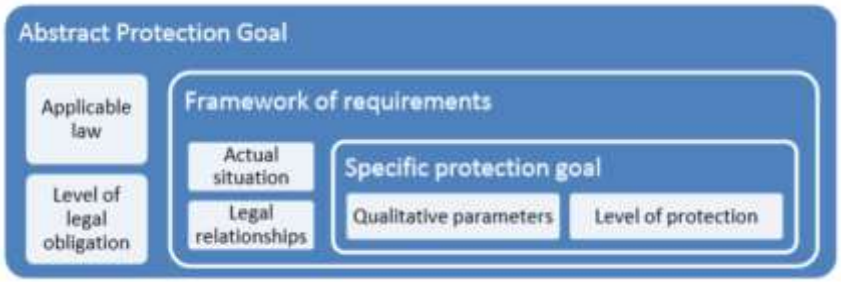
157 The Standard Data Protection Model



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



https://www.datenschutzzentrum.de/sdm/

158 Руководство по защите данных для архивных служб от EAG



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.

https://ec.europa.eu/info/about-european-commission/service-standards-and-principles/transparency/freedom-information/access-documents/information-and-document-management/archival-policy/european-archives-group_en

Псевдонимизация и анонимизация

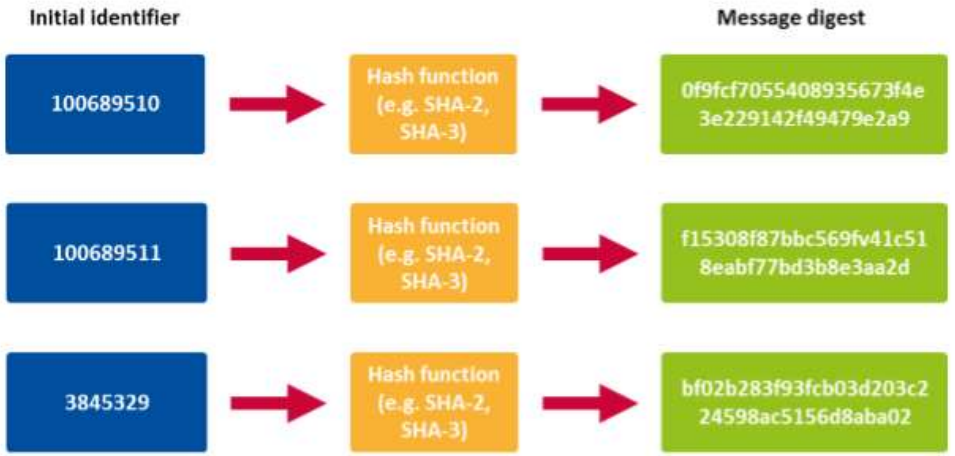


К оглавлению

Обзор концепции и реализации методов псведонимизации данных от ENISA

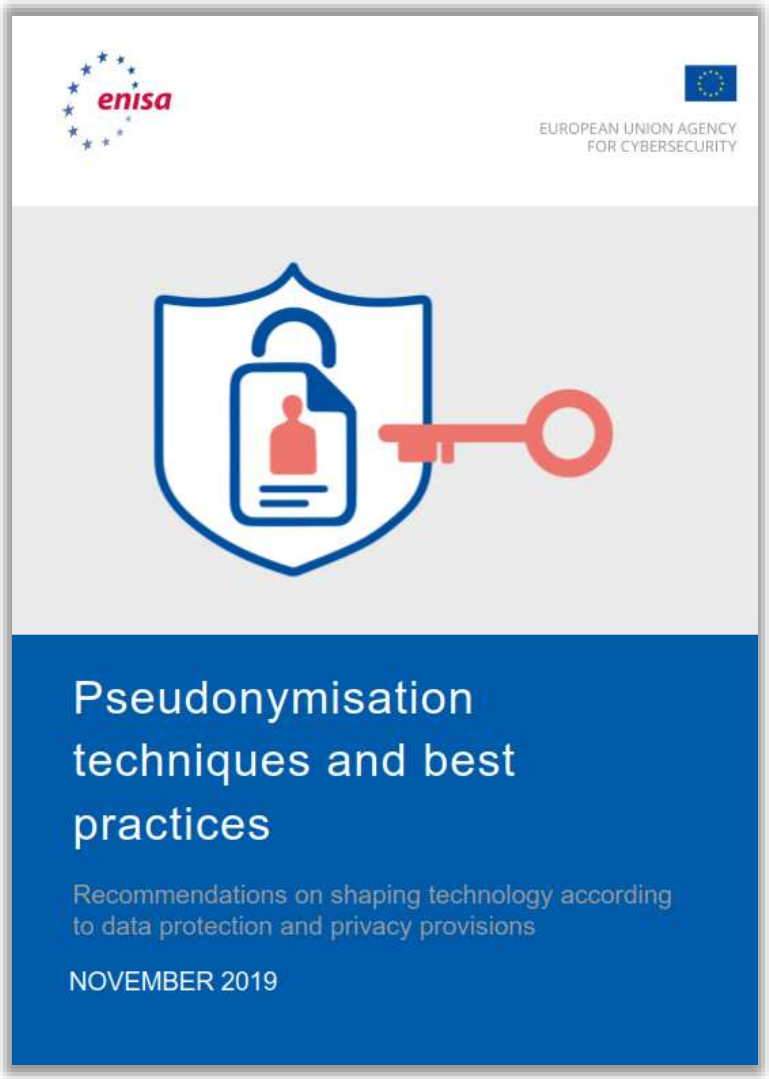


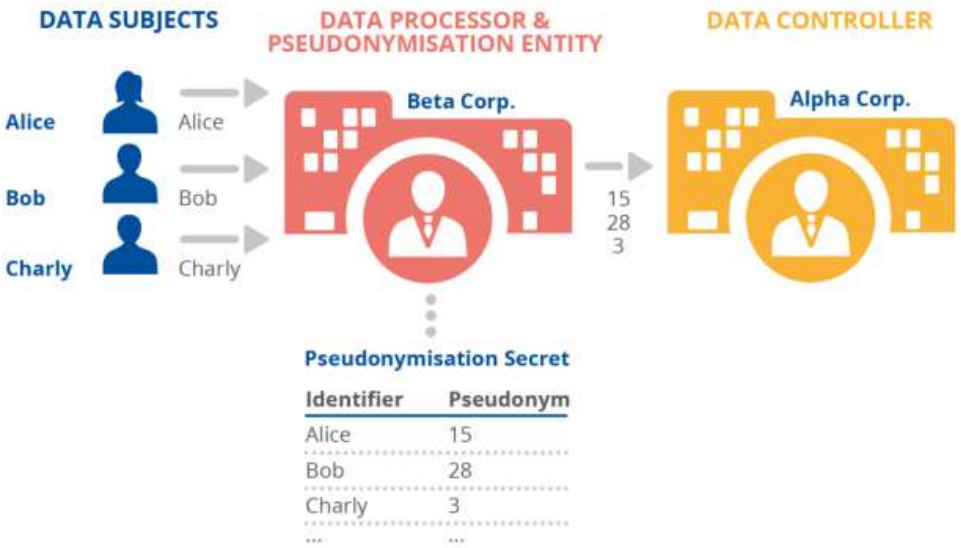
Целью данного обзора является изучение как концепции псевдонимизации, так практической реализации различных методов псевдонимазации данных. Обзор сосредоточен на анализе технических решений для выполнения требований GDPR в части защиты персональных данных и применения концепта «privacy by design».

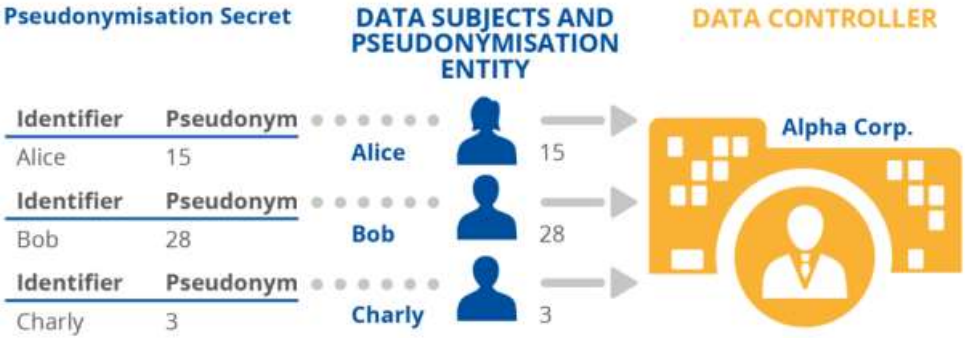


https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions

Рекомендации по техникам псведонимизации и лучшим практикам от ENISA

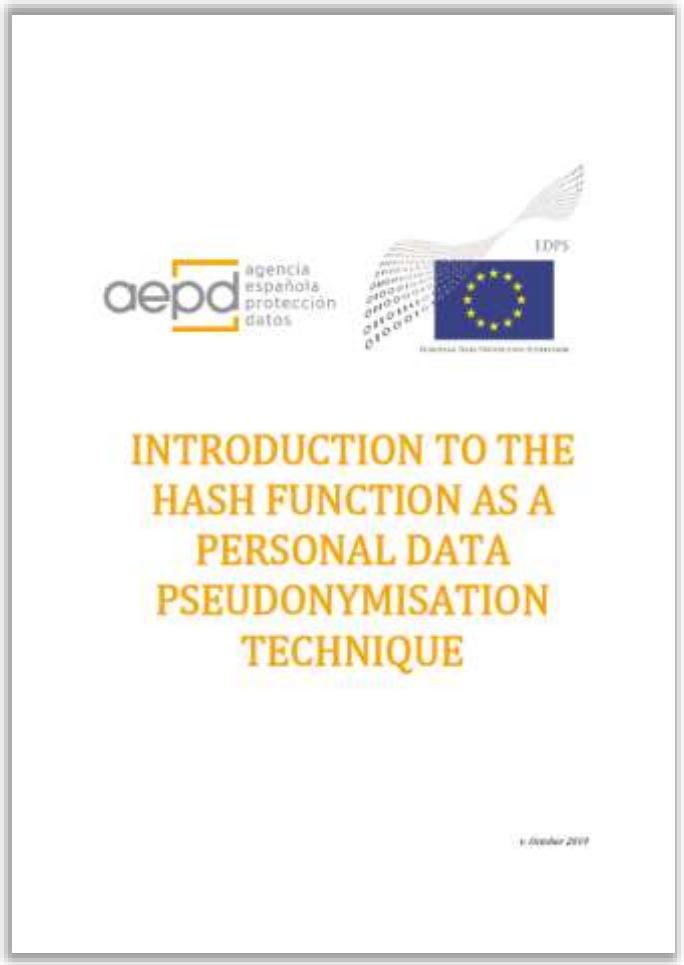


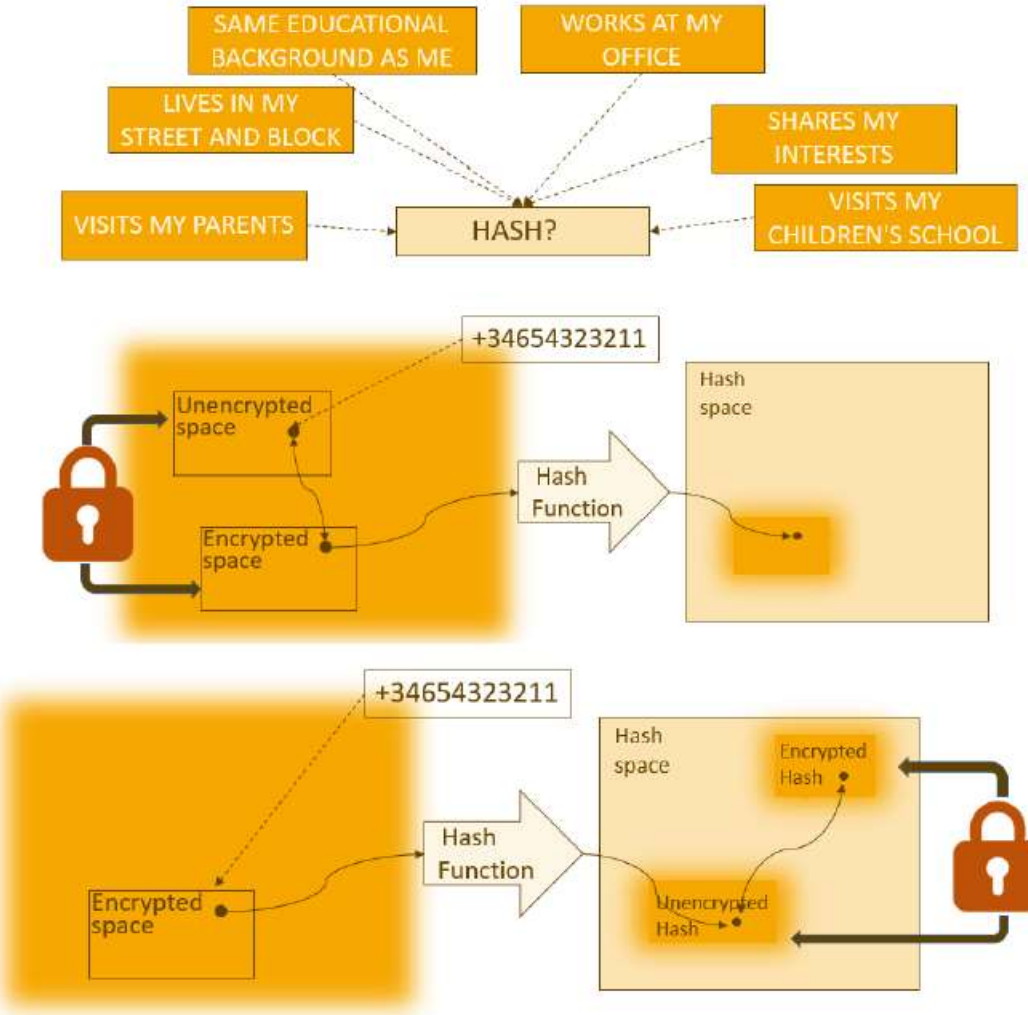




https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/at_download/fullReport

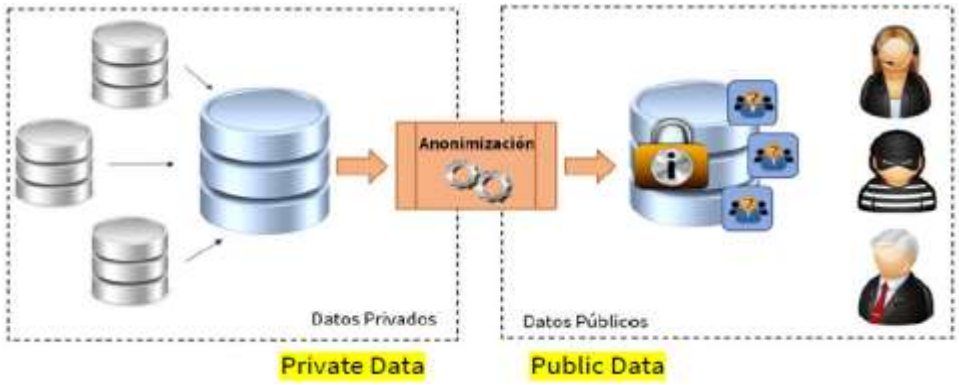
Руководство от AEPD и EDPS по использованию хеширования в псевдонимизации данных





https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf

Руководство от AEPD по K-анонимности как способе обеспечения конфиденциальности



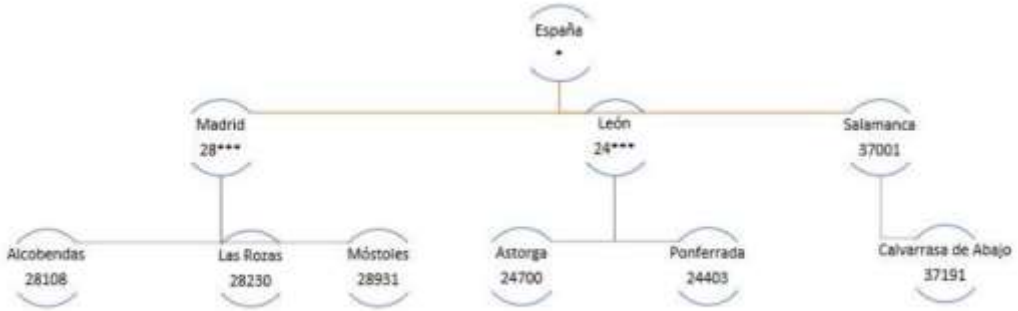


Figure 2: Hierarchy for the Postcode field

Postcode	Age	Cholesterol
37***	40 - 49	Y
28***	40 - 49	Y
24***	30 - 39	N
24***	30 - 39	N
37***	40 - 49	Y
28***	40 - 49	Y

Table 3 - Global generalisation

Postcode	Age	Cholesterol
37***	40 - 49	Y
28***	40 - 49	Y
24700	30 - 39	N
24700	30 - 39	N
37***	40 - 49	Y
28***	40 - 49	Y

Table 4 - Local generalisation

24700	37	N
24700	37	N
37003	44	Y
28108	40	Y
37891	33	N
50011	13	Y

Table 5: Table 2 expanded with data outside the range

Postcode	Age	Cholesterol
37003	40	Y
28108	44	Y
24700	37	N
24700	37	N
37003	44	Y
28108	40	Y
37891	33	N
50011	13	Y

Table 5: Original

Postcode	Age	Cholesterol
37***	40 - 49	Y
28***	40 - 49	Y
24700	30 - 39	N
24700	30 - 39	N
37***	40 - 49	Y
28***	40 - 49	Y
37***	30 - 39	N

Table 6: Generalisation + Suppression on Table 5

https://www.aepd.es/sites/default/files/2019-12/nota-tecnica-kanonimidad-en.pdf

Руководство от BfDI о правовых аспектах анонимизации данных с особым вниманием к телеком отрасли



BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Bonn, den 10. Februar 2020

Öffentliches Konsultationsverfahren

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Thema:

Anonymisierung unter der DSGVO

unter besonderer Berücksichtigung der TK-Branche

Das Konsultationsverfahren richtet sich insbesondere an Akteure aus Politik, Wirtschaft, Gesellschaft und Verwaltung, die sich diesem Thema befassen.

Kommentare und Stellungnahmen können bis einschließlich 09. März 2020 an die an E-Mail-Adresse

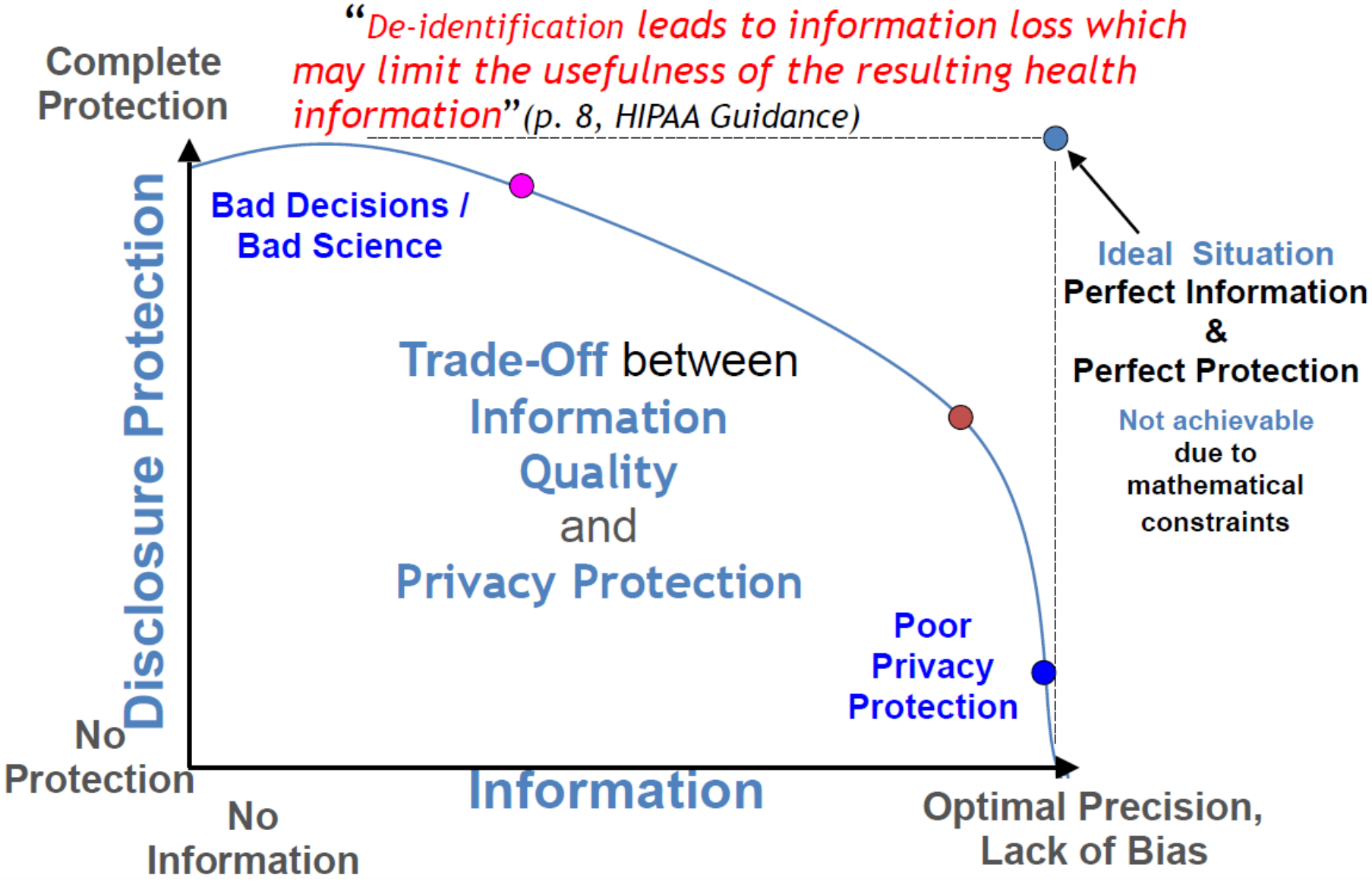
konsultation@bfdi.bund.de

geschickt werden.

Федеральный комиссар по защите данных и свободе информации в ФРГ 10.02.2020 опубликовал проект руководства о правовых аспектах анонимизации данных с особым вниманием к телеком отрасли. Публичные консультации продлятся до 09.03.2020. В частности, руководство анализирует различные правовое основы для анонимизации персональных данных в зависимости от контекста и цели анонимизации.

https://www.bfdi.bund.de/SharedDocs/Konsultationsverfahren/2020/01_Anonymisierung-TK.pdf?__blob=publicationFile&v=6

Презентация по деидентификации и реидентификации согласно стандарту NISTIR 8053



https://www.nist.gov/system/files/documents/itl/iad/vug/2016-03-07-De-IDv5-2.pdf

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

Data situation audit

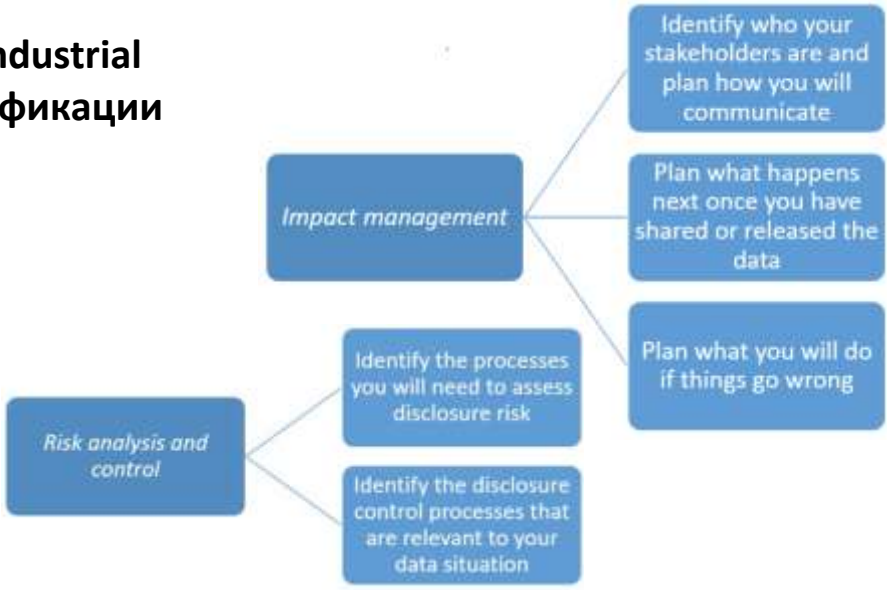
1. Describe your data situation
2. Understand your legal responsibilities
3. Know your data
4. Understand the use case
5. Meet your ethical obligations

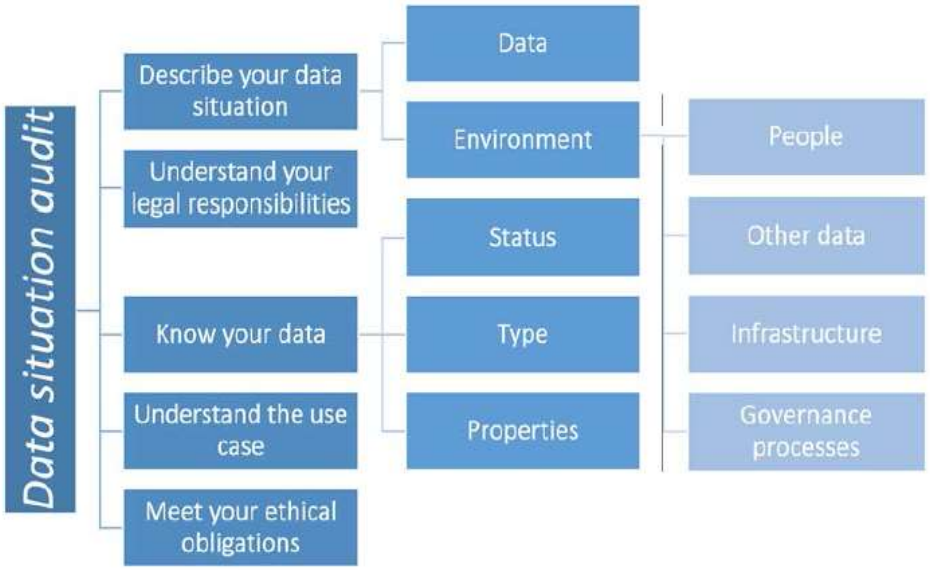
Risk analysis and control

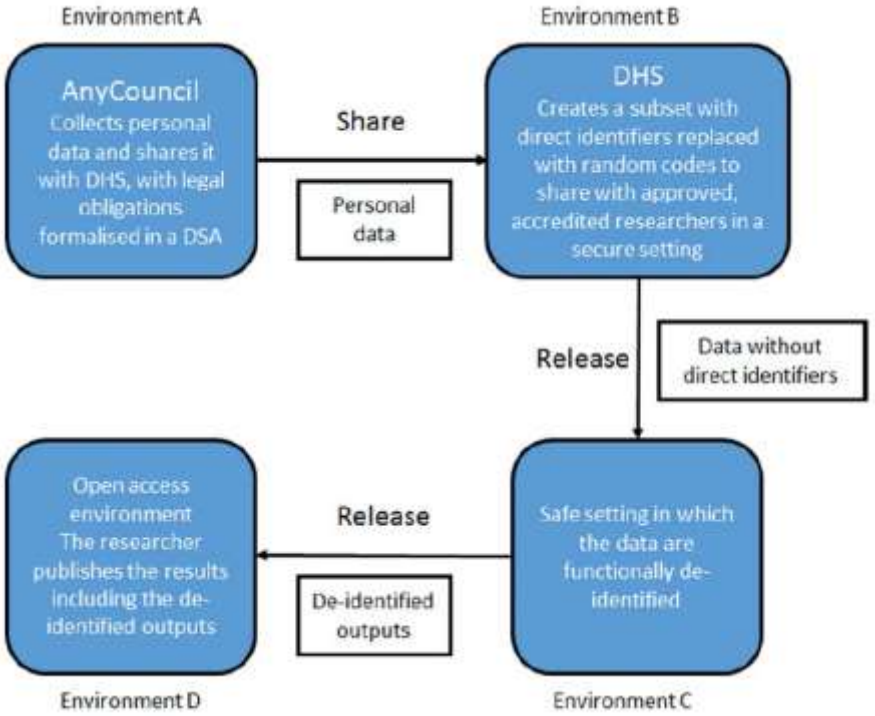
6. Identify the processes you will need to assess disclosure risk
7. Identify the disclosure control processes that are relevant to your data situation

Impact management

8. Identify who your stakeholders are and plan how you will communicate
9. Plan what happens next once you have shared or released the data
10. Plan what you will do if things go wrong

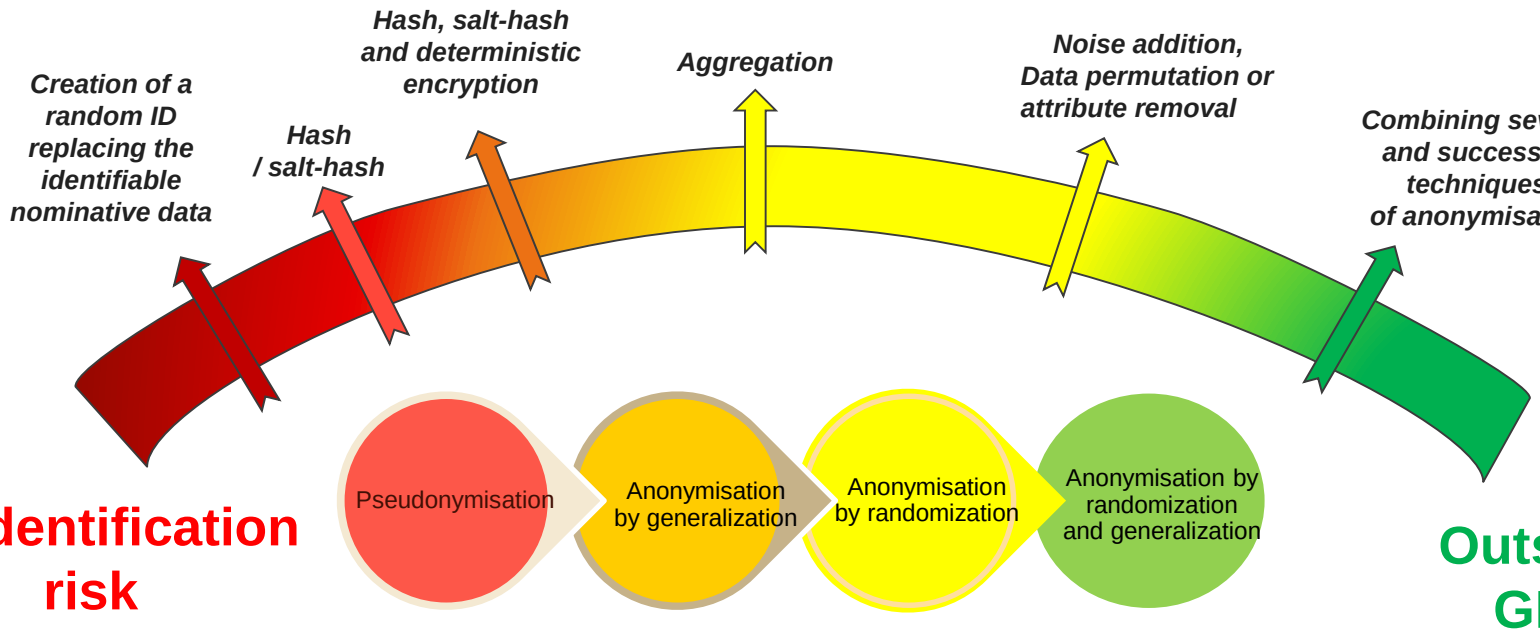






https://data61.csiro.au/en/Our-Research/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework

WHAT IS NOT PERSONAL DATA: ANONYMISATION



Re-identification risk

Outside of GDPR scope

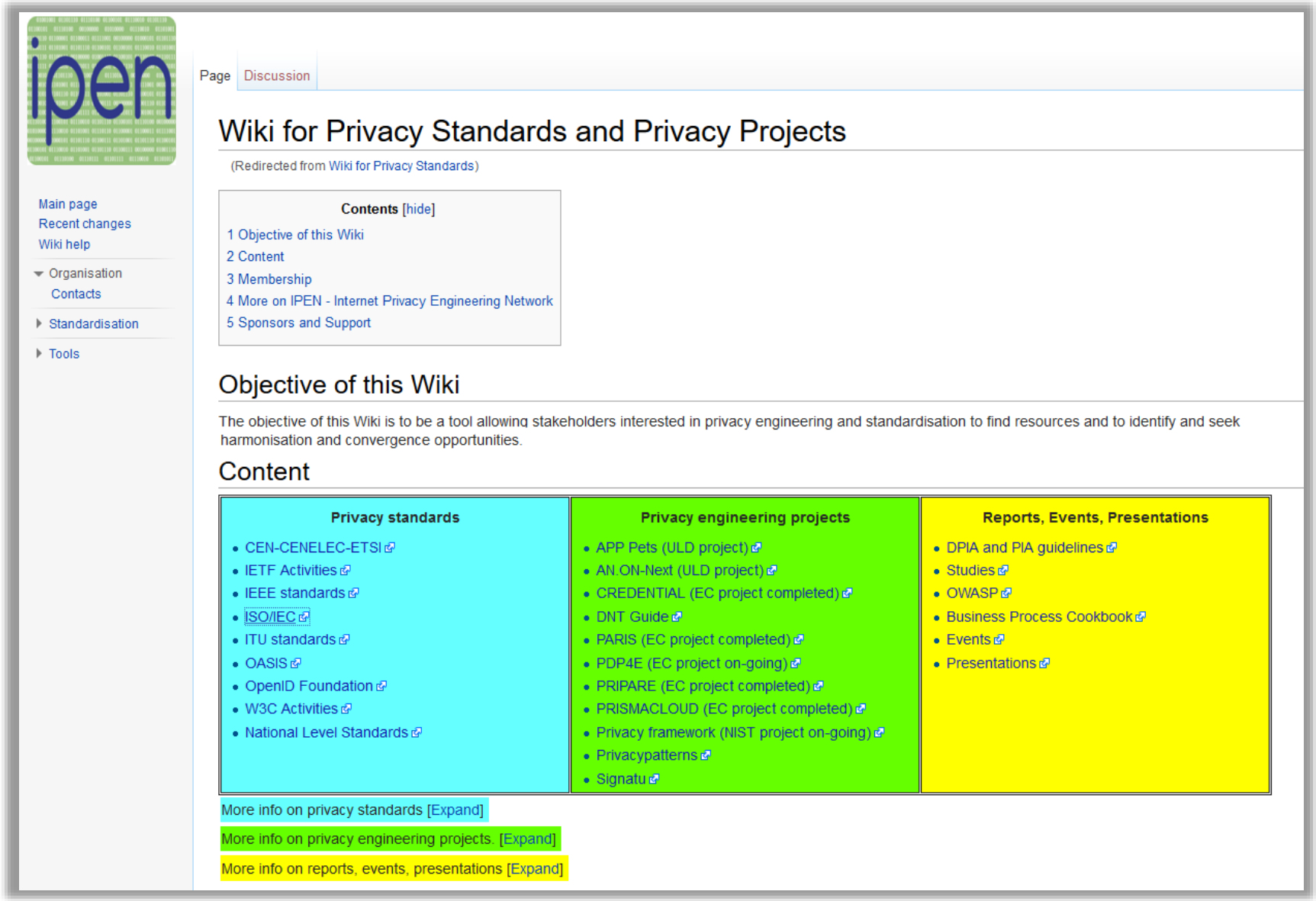
Pseudonymized data are still personal data

Международные стандарты



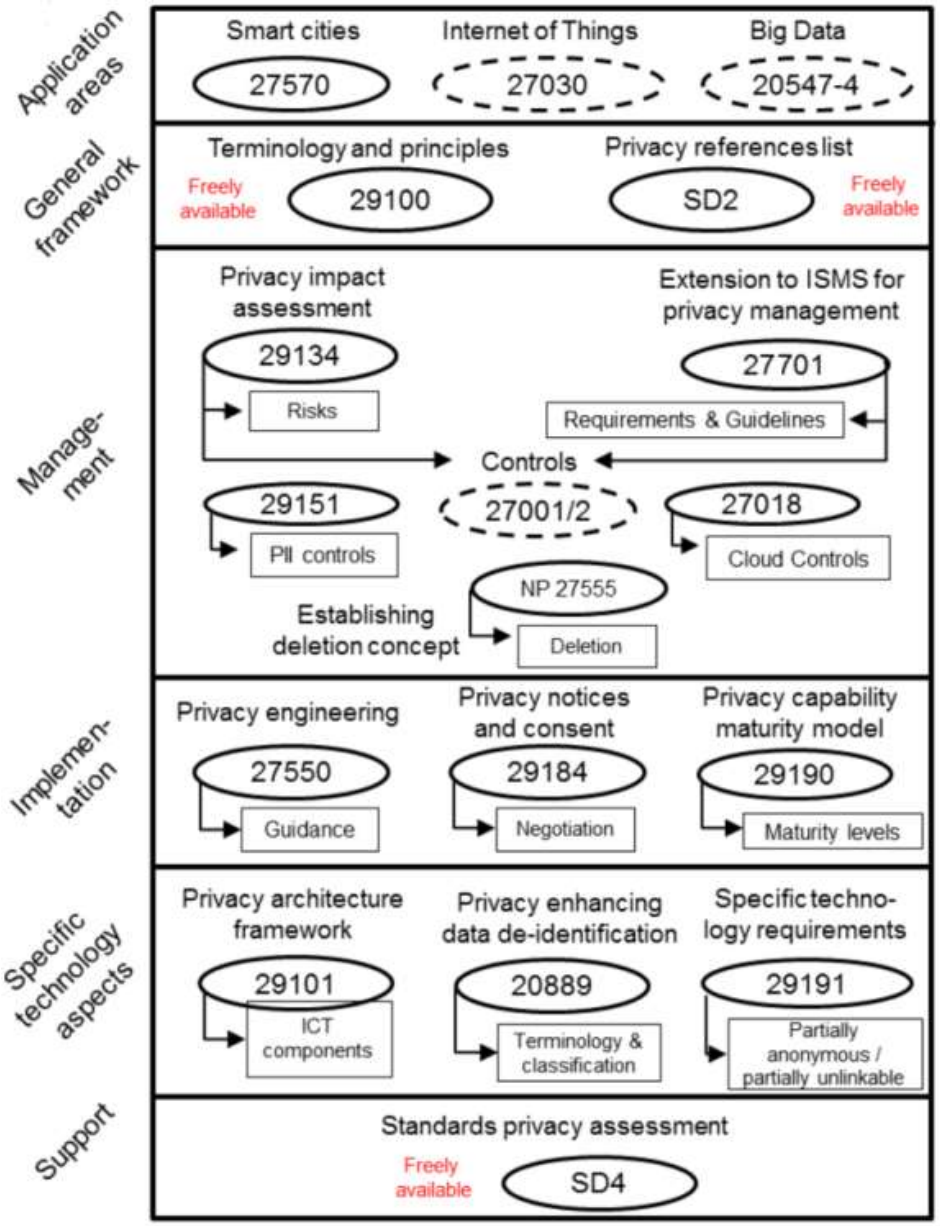
К оглавлению

Обзор стандартов и проектов в сфере Privacy от IPEN (Internet Privacy Engineering Network)



https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards

170 Обзор стандартов ISO в сфере Privacy



https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201901/Documents/Antonio_Kung_Presentation.pdf

Стандарт ISO/IEC 27001:2013. Системы Менеджмента Информационной Безопасности. Требования



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).

https://www.iso.org/standard/54534.html

Стандарт ISO/IEC 27017:2015. Защита персональных данных при предоставлении облачных услуг


INTERNATIONAL STANDARD

ISO/IEC 27017

First edition
2015-12-15

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Reference number
ISO/IEC 27017:2015(E)

ISO IEC

© ISO/IEC 2015

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.

https://www.iso.org/standard/43757.html

Стандарт ISO/IEC 27018:2019. Практика защиты персональных данных в публичных облаках



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 27018:2019 «Информационные технологии - Методы обеспечения безопасности - Практика защиты персональных данных в публичных облаках, выступающих в роли обработчиков персональных данных» (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).

Стандарт устанавливает общепринятые цели управления, меры и средства управления и даёт рекомендации по реализации мер по защите персональных данных (Personally Identifiable Information, PII) в соответствии с принципами защиты неприкосновенности частной жизни, сформулированными в стандарте ISO/IEC 29100, для среды облачных вычислений в публичных облаках.

https://www.iso.org/standard/76559.html

Стандарт ISO/IEC 27701:2019. Расширение до ISO/IEC 27001 и ISO/IEC 27002 по управлению персональными данными


INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

ISO IEC

Reference number
ISO/IEC 27701:2019(E)

© ISO/IEC 2019

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 операторов (controllers) и обработчиков (processors) в отношении обработки персональных данных.

https://www.iso.org/standard/71670.html

Стандарт ISO/IEC 27750:2019. Инженерия обеспечения неприкосновенности частной жизни



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт 27750:2019 «Информационная безопасность - Меры безопасности - Инженерия обеспечения неприкосновенности частной жизни» (Information technology - Security techniques - Privacy engineering).

В стандарте описаны рекомендации по запроектированной 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.

https://www.iso.org/standard/72024.html

Стандарт ISO/IEC 27102:2019. Руководство по киберстрахованию


INTERNATIONAL STANDARD

ISO/IEC 27018

Second edition
2019-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

ISO IEC

Reference number
ISO/IEC 27018:2019(E)

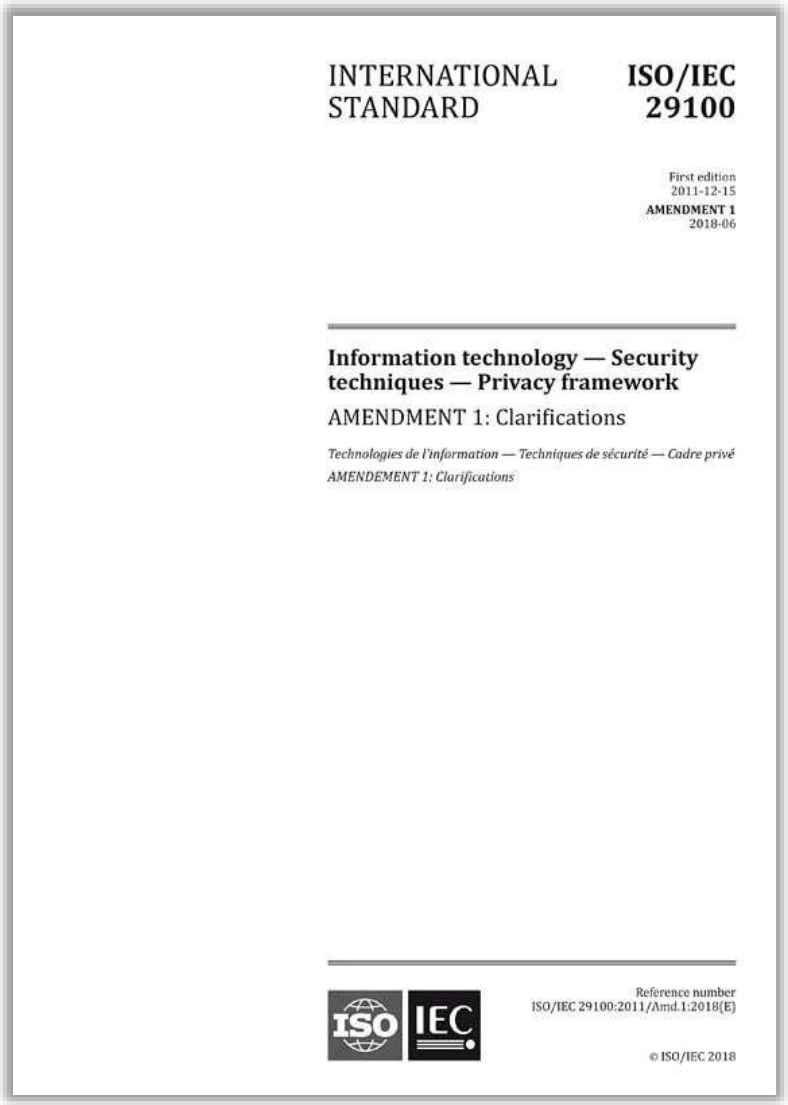
© ISO/IEC 2019

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 кибер-инцидента в рамках используемой организацией системы менеджмента рисков информационной безопасности.

https://www.iso.org/standard/72436.html

Стандарт ISO/IEC 29100:2018. Концепция защиты персональных данных



INTERNATIONAL STANDARD

ISO/IEC 29100

First edition
2011-12-15
AMENDMENT 1
2018-06

Information technology — Security techniques — Privacy framework

AMENDMENT 1: Clarifications

Technologies de l'information — Techniques de sécurité — Cadre privé
AMENDEMENT 1: Clarifications

Reference number
ISO/IEC 29100:2011/Amd.1:2018(E)

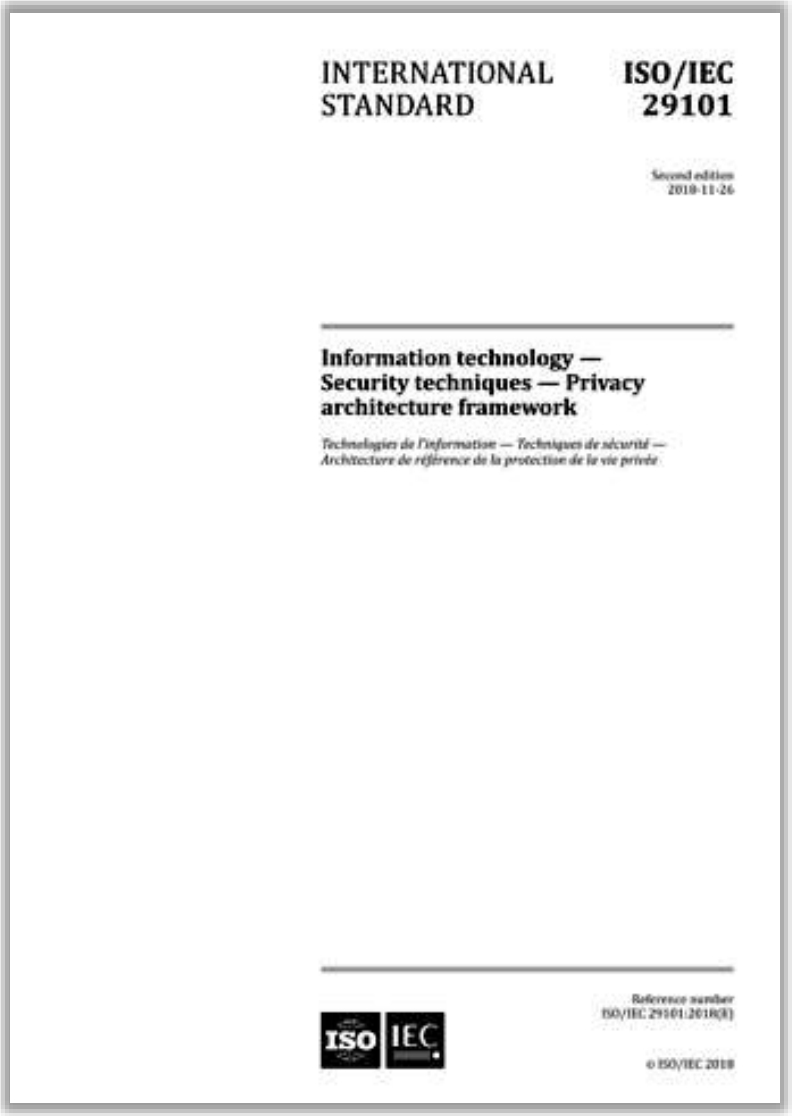
© ISO/IEC 2018

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».

https://www.iso.org/standard/45123.html

Стандарт ISO/IEC 29101:2018. Концепция архитектуры, обеспечивающей защиту персональных данных



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 29101:2018 «Информационная безопасность – Меры безопасности – Концепция архитектуры, обеспечивающей защиту персональных данных» (Information technology - Security techniques - Privacy architecture framework).

В стандарте описаны высокоуровневая концепция архитектуры и взаимосвязанные с ней меры контроля и управления, используемые для защиты неприкосновенности частной жизни (персональных данных) в ИКТ-системах, которые хранят и обрабатывают персональные данные.

https://www.iso.org/standard/45124.html

Стандарт ISO/IEC 29134:2017. Оценка воздействия на неприкосновенность частной жизни


INTERNATIONAL STANDARD

ISO/IEC 29134

First edition
2017-06

Information technology — Security techniques — Guidelines for privacy impact assessment

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'évaluation d'impacts sur la vie privée

ISO IEC

Reference number
ISO/IEC 29134:2017(E)

© ISO/IEC 2017

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 проведений «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 разнобой 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.

https://www.iso.org/standard/62289.html

Стандарт ISO/IEC 29151:2017. Свод практики по защите персональных данных



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

Стандарт является непосредственным дополнением действующего стандарта ISO/IEC 27018:2014 «Информационные технологии - Методы обеспечения безопасности – Практика защиты персональных данных в публичных облаках, выступающих в роли обработчиков персональных данных» (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).

https://www.iso.org/standard/62726.html

Стандарт ISO/IEC 29190:2015. Оценка способности обеспечить неприкосновенность частной жизни


INTERNATIONAL STANDARD

ISO/IEC 29190

First edition
2015-08-15

Information technology — Security techniques — Privacy capability assessment model

Technologies de l'information — Techniques de sécurité — Modèle d'évaluation de l'aptitude à la confidentialité

Reference number
ISO/IEC 29190:2015(E)

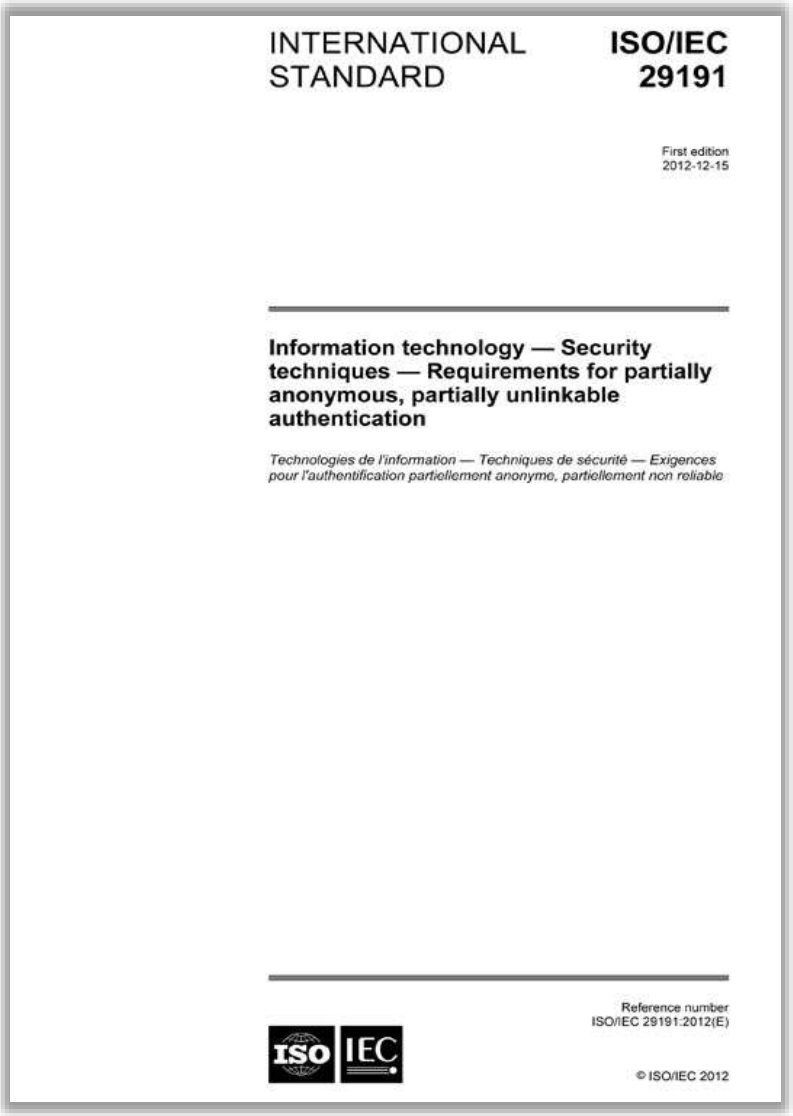
© ISO/IEC 2015

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.

https://www.iso.org/standard/45269.html

Стандарт ISO/IEC 29191:2012. Требования к частично анонимной и частично несвязываемой аутентификации


INTERNATIONAL STANDARD

ISO/IEC 29191

First edition
2012-12-15

Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication

Technologies de l'information — Techniques de sécurité — Exigences pour l'authentification partiellement anonyme, partiellement non reliable

Reference number
ISO/IEC 29191:2012(E)

© ISO/IEC 2012

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.

https://www.iso.org/standard/45270.html

Стандарт ISO/IEC 20889:2018. Обезличивание персональных данных



Международной организацией по стандартизации (International Organization for Standardization) был опубликован стандарт ISO/IEC 20889:2018 «Терминология и классификация методов де-идентификации (обезличивания) данных с целью усиления защиты неприкосновенности частной жизни (персональных данных)» (Privacy enhancing data de-identification terminology and classification of techniques).

В стандарте описаны усиливающие защиту неприкосновенности частной жизни методы де-идентификации данных. Стандарт предназначен для использования при описании и проектировании мер по де-идентификации в соответствии с принципами защиты неприкосновенности частной жизни, сформулированными в стандарте ISO/IEC 29100:2011 «Информационная технология. Методы и средства обеспечения безопасности. Концепция защиты персональных данных» (Information technology - Security techniques - Privacy framework).

https://www.iso.org/ru/standard/69373.html

Технические спецификации ISO/IEC TS 20748-4:2019. Защита персональных данных в сфере образования

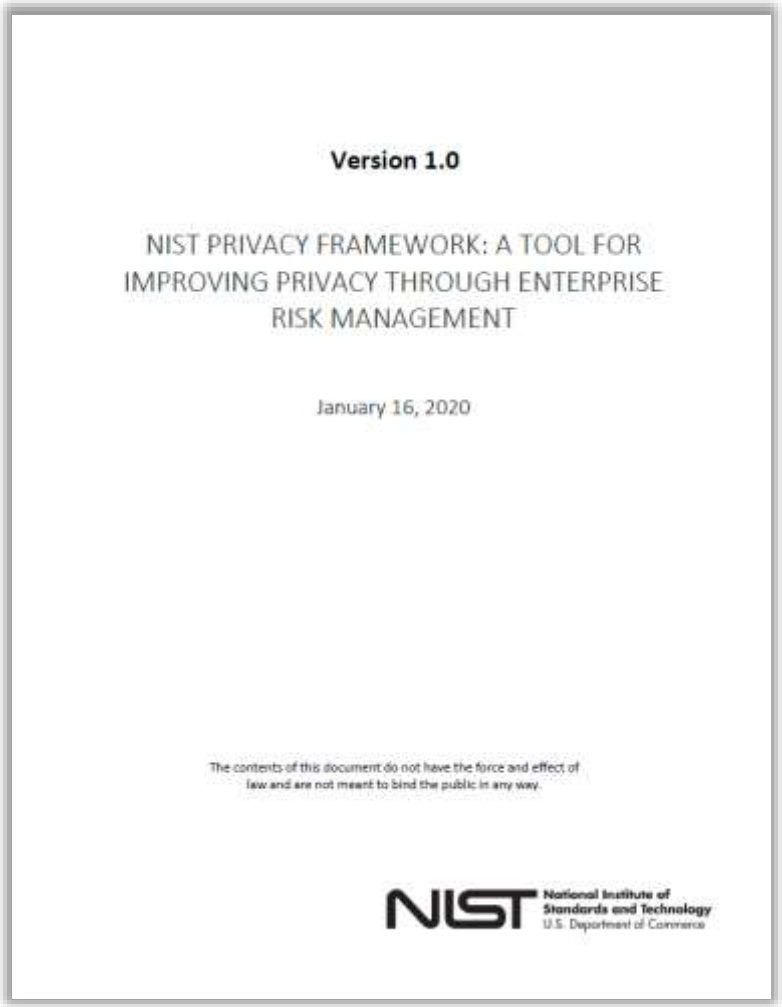


Международной организацией по стандартизации (International Organization for Standardization) был опубликован технические спецификации ISO/IEC TS 20748-4:2019 «Информационные технологии для обучения, образования и подготовки - Интероперабельность средств сбора и обработки данных об учащихся - Часть 4: 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).

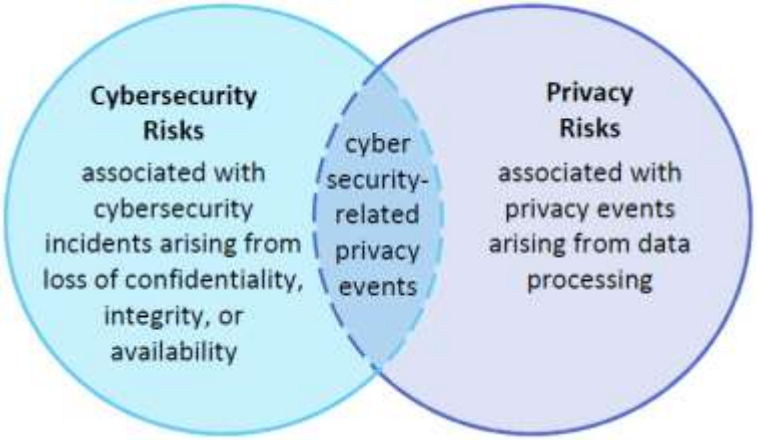
В документе устанавливаются требования к защите неприкосновенности частной жизни и персональных данных, которые должны использоваться при проектировании систем сбора и обработки данных об учащихся (learning analytics) и в практике сбора и обработки такого рода данных в школах, университетах, при обучении на рабочем месте и при использовании смешанных подходов к обучению.

https://www.iso.org/standard/74379.html

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







https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

186 Другие стандарты по защите персональных данных (1)

ISO/IEC 15944-8:2012 «Информационные технологии – Взгляд с точки зрения деловых операций. Часть 8. Выявление требований к защите персональных данных в качестве внешних ограничений на деловые операции» (Information technology - Business operational view - Part 8: Identification of privacy protection requirements as external constraints on business transactions) https://www.iso.org/standard/51544.html

ISO/IEC 29187-1:2013 «Информационные технологии – Выявление требований к защите персональных данных, относящихся к обучению, образованию и тренировке (LET). Часть 1: Концепция и эталонная модель» (Information technology - Identification of privacy protection requirements pertaining to learning, education and training (LET) - Part 1: Framework and reference model) https://www.iso.org/standard/45266.html

ISO 22307:2008 «Финансовые услуги – Оценка воздействия на неприкосновенность частной жизни» (Financial services - Privacy impact assessment) https://www.iso.org/standard/40897.html

ISO/TS 17975:2015 «Информатика в здравоохранении - Принципы и требования к данным для согласия на сбор, использование или раскрытие персональной информации о здоровье» (Health informatics - Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information) https://www.iso.org/standard/61186.html

ISO 22857:2013 «Информатика в здравоохранении – Руководство по защите персональных данных с целью содействия трансграничной передаче персональной информации о здоровье» (Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health data) https://www.iso.org/standard/52955.html

ISO/TS 14441:2013 «Информатика в здравоохранении – Требования по безопасности и защите персональных данных к системам управления электронными медицинскими документами, для использования при оценке соответствия» (Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment) https://www.iso.org/standard/61347.html

ISO 25237:2017 «Информатизация здоровья. Псевдонимизация» (Health informatics - Pseudonymization) https://www.iso.org/standard/63553.html

ISO/TR 12859:2009 «Интеллектуальные транспортные системы (ИТС) - Архитектура систем - Вопросы защиты неприкосновенности частной жизни в стандартах и системах ИТС» (Intelligent transport systems - System architecture - Privacy aspects in ITS standards and systems) https://www.iso.org/standard/52052.html

187 Другие стандарты по защите персональных данных (2)

ISO 16461:2018 «Интеллектуальные транспортные системы (ИТС) – Критерии защиты целостности и защиты персональных данных в системах бортовых транспортных датчиков» (Intelligent transport systems - Criteria for privacy and integrity protection in probe vehicle information systems) https://www.iso.org/standard/56791.html

ISO/TR 17427-7:2015 «Интеллектуальные транспортные системы (ITS) - Кооперативные ITS. Часть 7. Вопросы защиты неприкосновенности частной жизни» (Intelligent transport systems - Cooperative ITS - Part 7: Privacy aspects) https://www.iso.org/standard/66959.html

ISO/IEC TS 19608:2018 «Руководство по разработке функциональных требований к безопасности и защите персональных данных на основе ISO/IEC 15408» (Guidance for developing security and privacy functional requirements based on ISO/IEC 15408) https://www.iso.org/standard/65459.html

ISO/IEC 19086-4:2019 « Облачные вычисления - Концепция соглашений о качестве услуг (SLA) - Часть 4: Компоненты безопасности и защиты персональных данных» (Cloud computing - Service level agreement (SLA) framework - Part 4: Components of security and of protection of PII) https://www.iso.org/standard/68242.html

BS 10012:2017 «Защита персональных данных - Спецификации для системы менеджмента персональной информации» (Data protection. Specification for a personal information management system) http://shop.bsigroup.com/ProductDetail/?pid=000000000030339453

NIST SP 800-53 «Меры обеспечения безопасности и защиты персональных данных, рекомендуемые для федеральных информационных систем и организаций» (Security and Privacy Controls for Federal Information Systems and Organizations) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.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

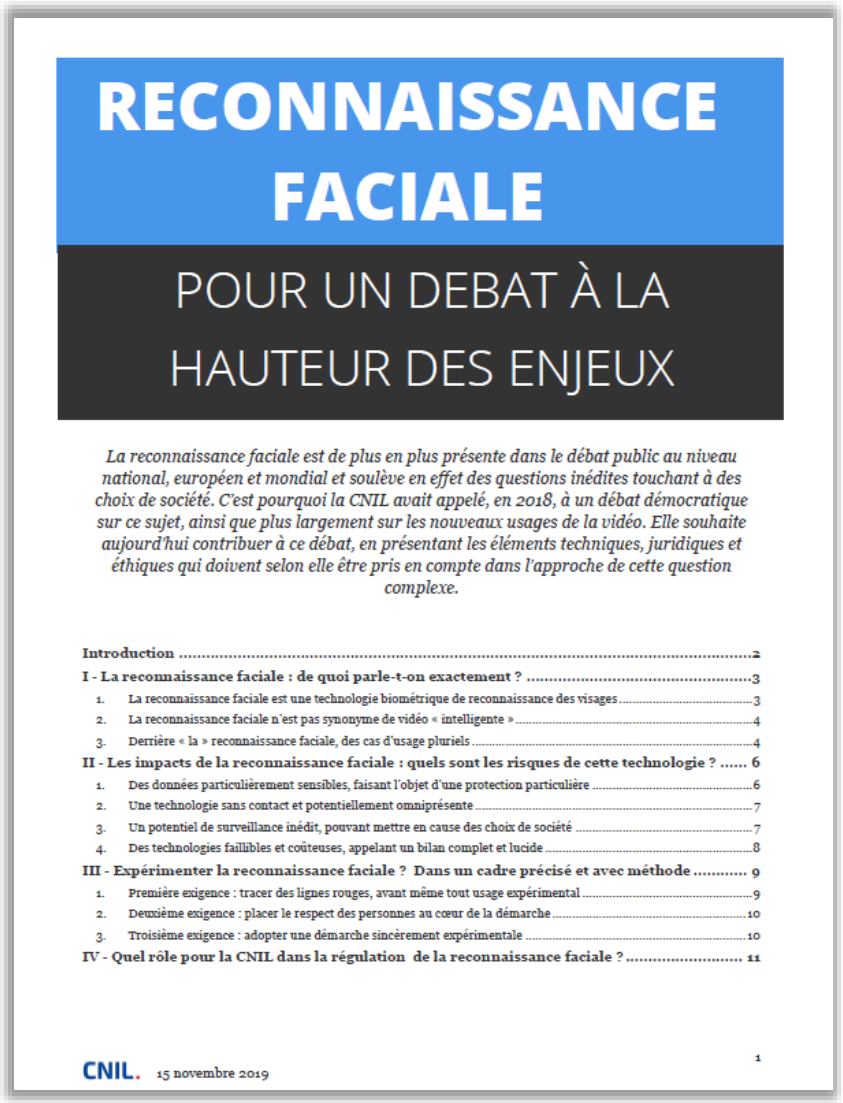
NIST SP 800-188 «Деидентификация государственных наборов данных» (De-Identifying Government Datasets) http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft2.pdf

Правоприменительная практика



К оглавлению

Отчет CNIL об использовании технологий распознавания лиц



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 précisé 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

CNIL. 15 novembre 2019

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 распознания лиц, которые должны соблюдаться при создании новых устройств.

https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

190 Договор между совместными контролерами



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.

https://www.cpdp.bg/?p=element_view&aid=2119



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

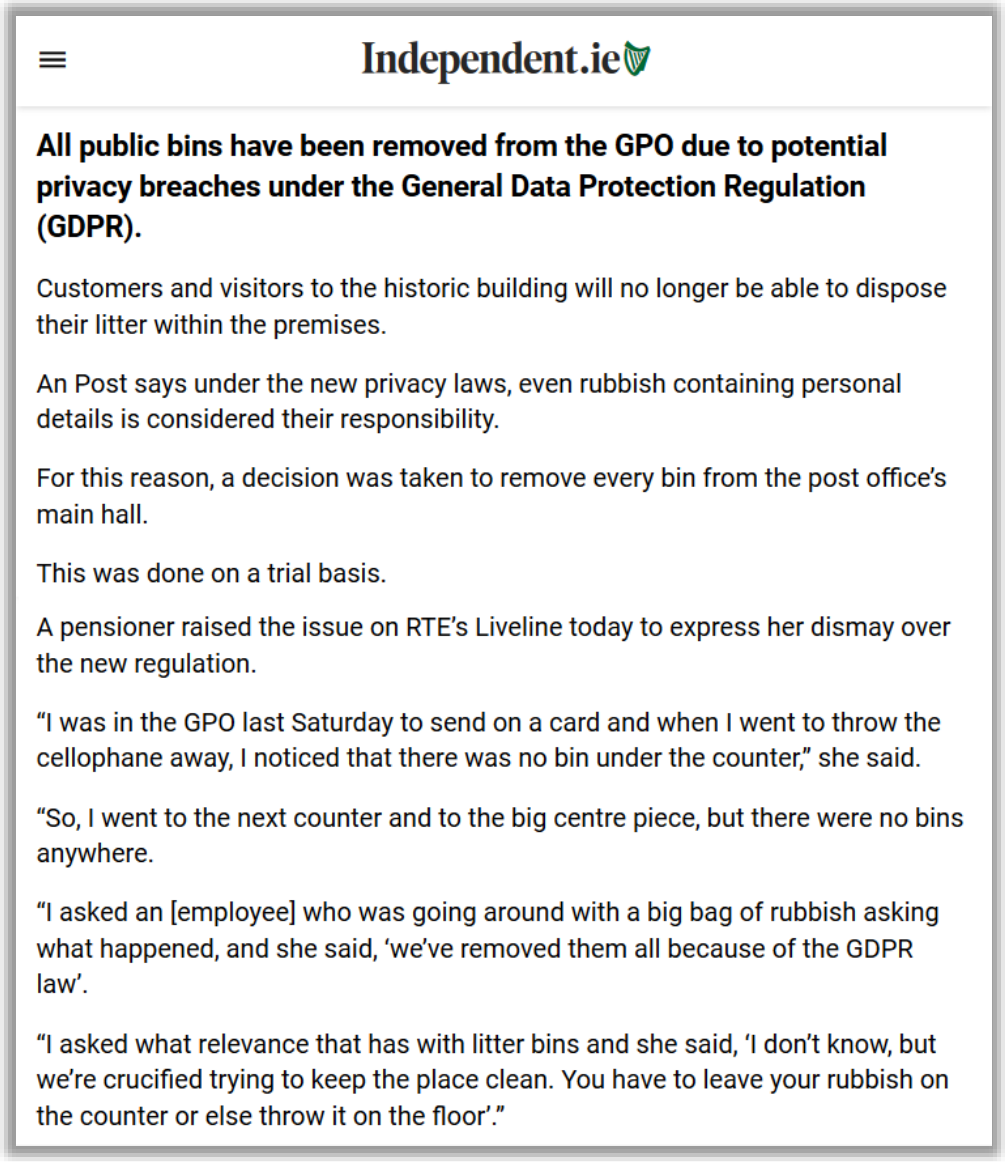
Decisions on the GDPR (from supervisory authorities and courts) are still rare and therefore I am always very pleased when such a decision, in which the new European law is applied and interpreted, sees the light of day.

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.

https://www.delegedata.de/2018/11/austrian-data-protection-authority-data-subjects-have-no-right-to-demand-implementation-of-certain-data-protection-measures-under-gdpr/

192 Ирландская почта убрала мусорные урны «из-за GDPR»



Independent.ie

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'."

The Irish Post

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.

https://amp.independent.ie/irish-news/news/public-bins-removed-from-the-gpo-over-gdpr-concerns-38073403.html

193 Отчет CNIL о GDPR и использовании технологии блокчейн

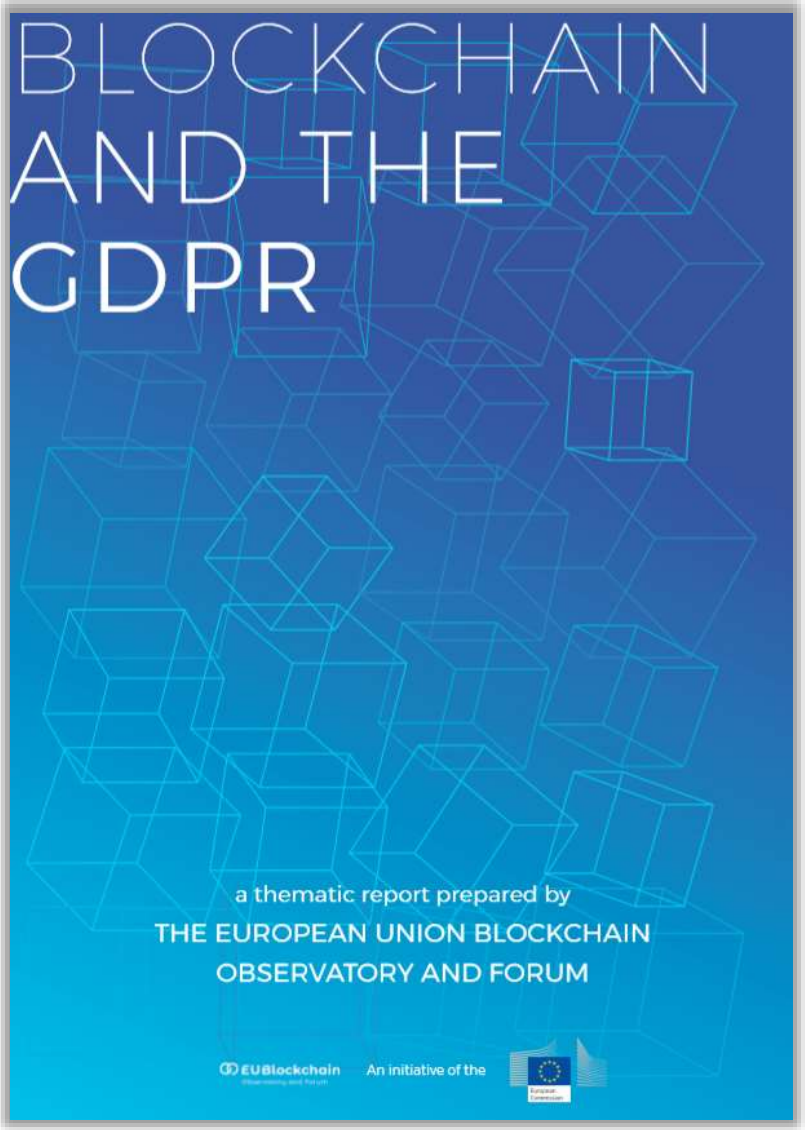


Commission nationale de l'informatique et des libertés

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

https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

Отчет о блокчейне и GDPR от European Union Blockchain Observatory & Forum



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

EUBlockchain Observatory and Forum

https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

Комиссар по защите данных Нижней Саксонии опубликовал сводный отчет по проверке 50 компаний

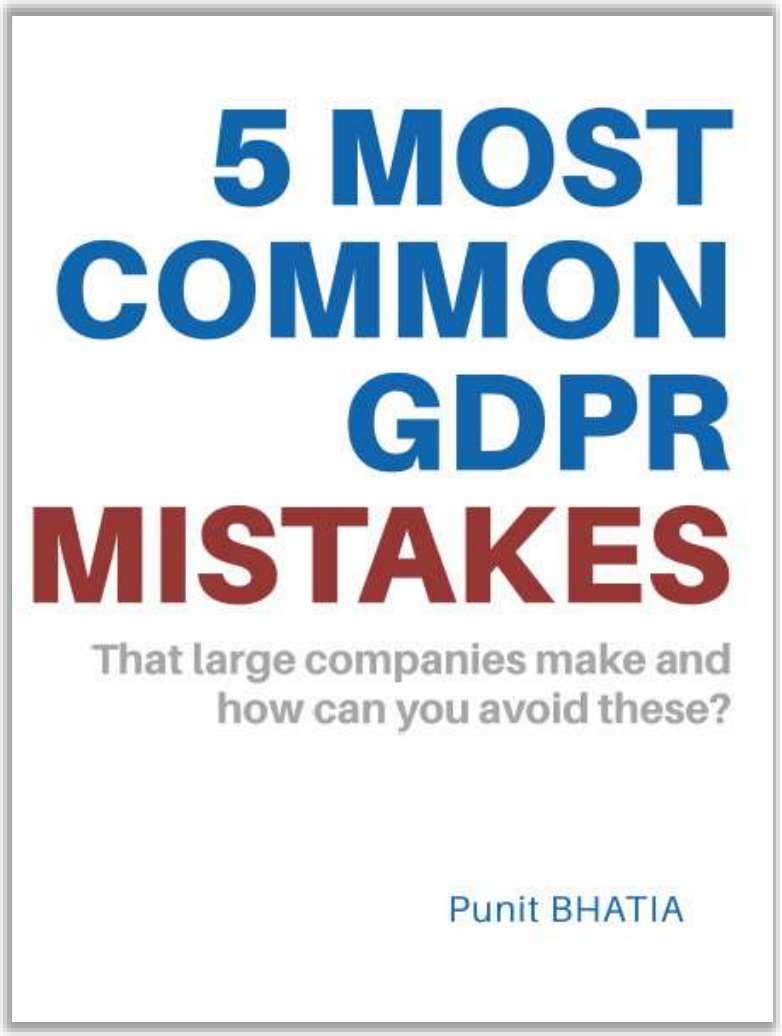


Государственный Комиссар по защите данных земли Нижняя Саксония (Die Landesbeauftragte für den Datenschutz Niedersachsen) опубликовал сводный отчет по проверке 50 компаний на соответствие GDPR, из которых продемонстрировали: удовлетворительный уровень – 9, неудовлетворительный уровень – 32, плохой уровень – 8. Некоторые выявленные недостатки:

- неприменение концептов Data protection by design and by default;
- не учитывались требования по проведению обязательного DPIA, не документировались решения об отсутствии необходимости проведения DPIA, недостаточное описание процессов обработки данных, недостаточный объем меры 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.

https://lfd.niedersachsen.de/download/149301

Пять самых распространённых и очевидных ошибок по GDPR по мнению 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.

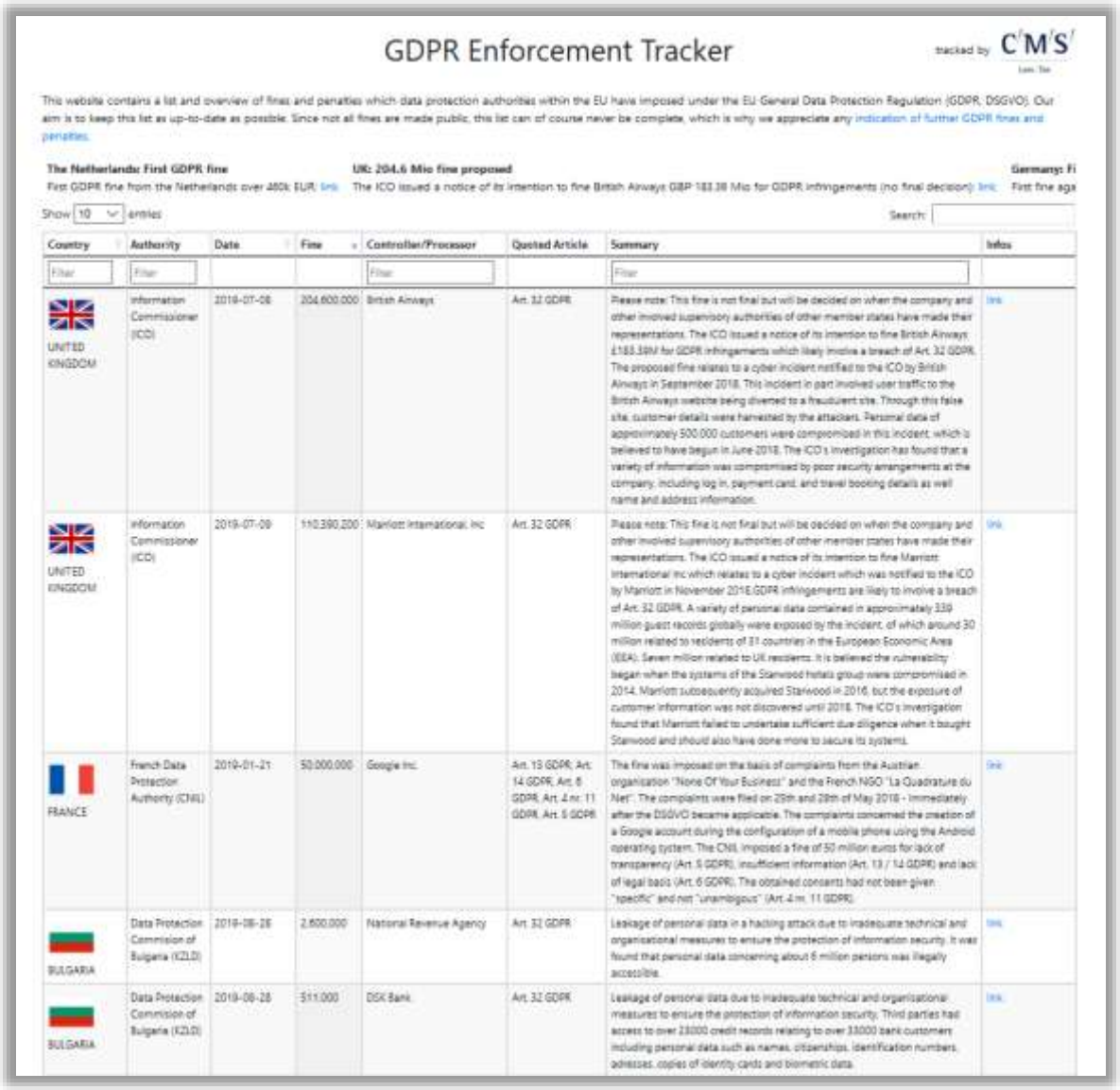
https://fit4gdpr.co.uk/

Штрафы - базы дел и аналитика



К оглавлению

198 База сведений о штрафов за нарушение GDPR



GDPR Enforcement Tracker

tracked by CMS

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 — First GDPR fine from the Netherlands over 460k EUR. link

UK: 204.6 Mio fine proposed — The ICO issued a notice of its intention to fine British Airways GBP 183.39 Mio for GDPR infringements (no final decision). link

Germany: Fi — First fine aga

Show 10 entries — Search:

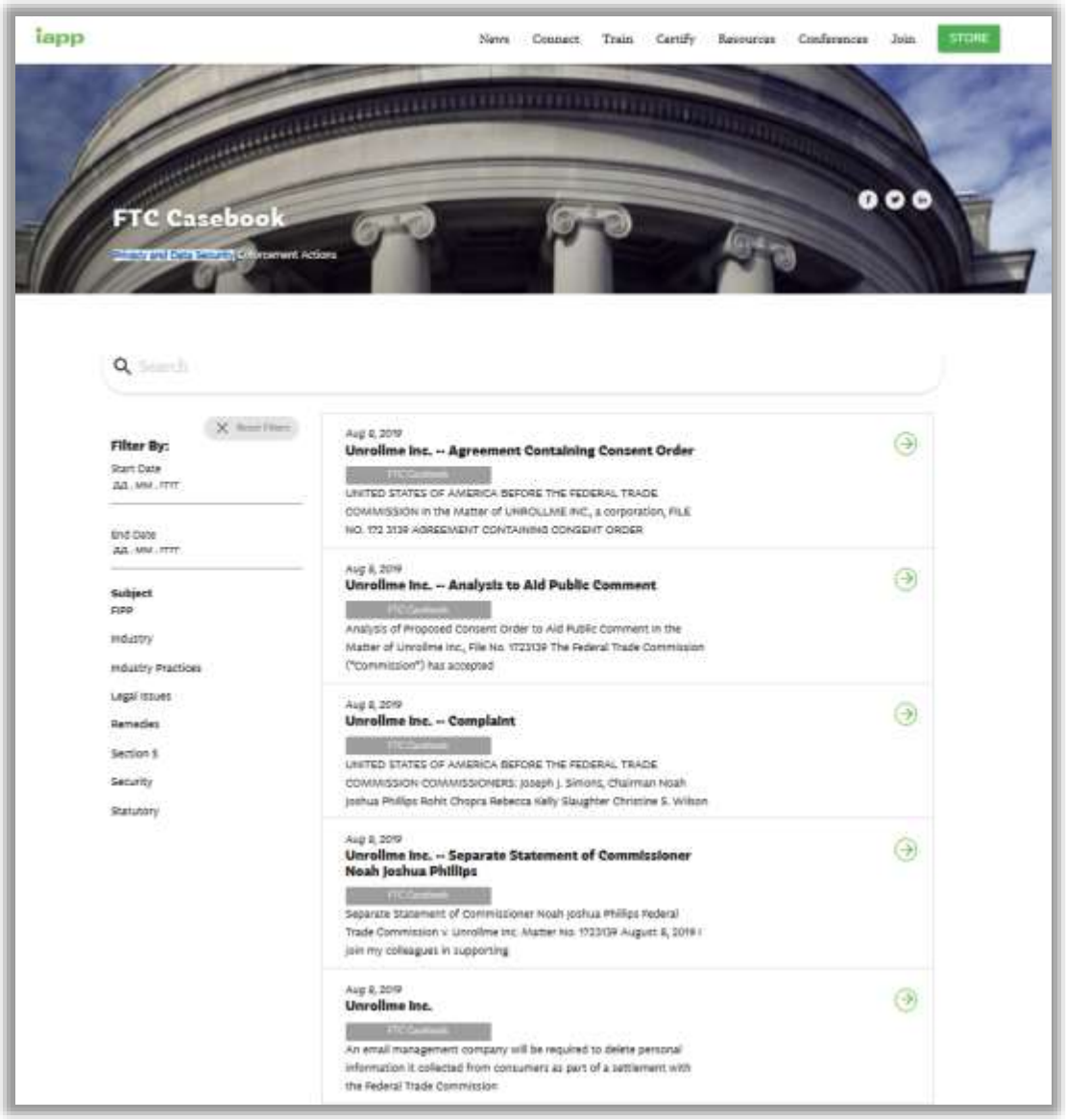
Country	Authority	Date	Fine	Controller/Processor	Quoted Article	Summary	Infos
UNITED KINGDOM	Information Commissioner (ICO)	2019-07-08	204.600.000	British Airways	Art. 32 GDPR	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other 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 Commision 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 Commision 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 33000 credit records relating to over 33000 bank customers including personal data such as names, citizenships, identification numbers, adresses, copies of identity cards and biometric data.	link

GDPR Enforcement Tracker

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

http://www.enforcementtracker.com/

База сведений о привлечении к ответственности за нарушение требований Privacy and Data Security



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.

https://iapp.org/resources/ftc-casebook

200 Аналитика KPMG по штрафам GDPR на 03.12.2019

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).

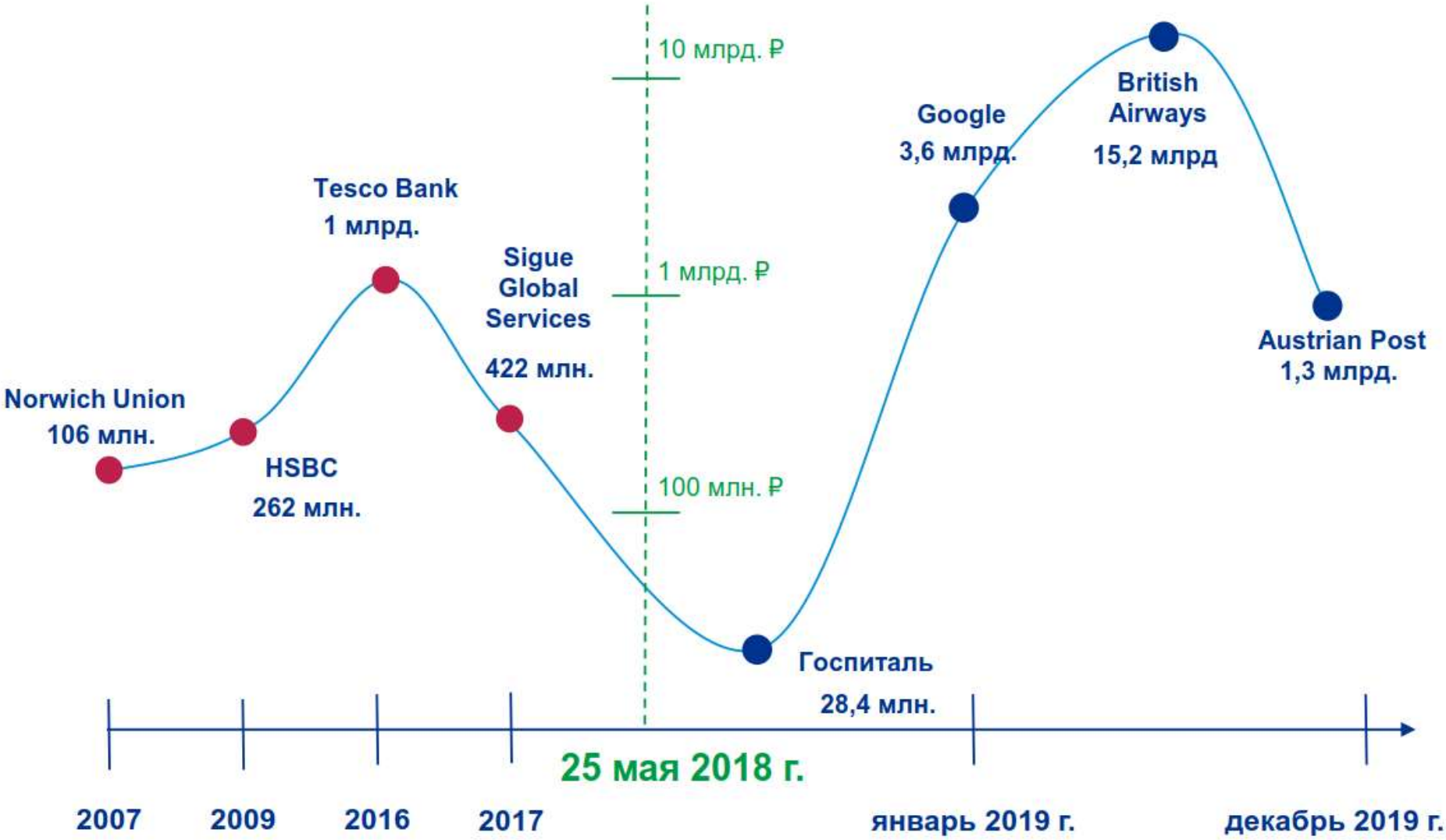
Курс валют*: по данным ЦБ на 03 декабря 2019 г.

* 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

http://rppa.ru/files/2019-12-03_gdpr.pdf

201 Аналитика KPMG по штрафам GDPR на 03.12.2019



http://rppa.ru/files/2019-12-03_gdpr.pdf

202 Аналитика KPMG по штрафам GDPR на 03.12.2019

Страны, входящие в ЕЭЗ, в которых зафиксированы штрафы

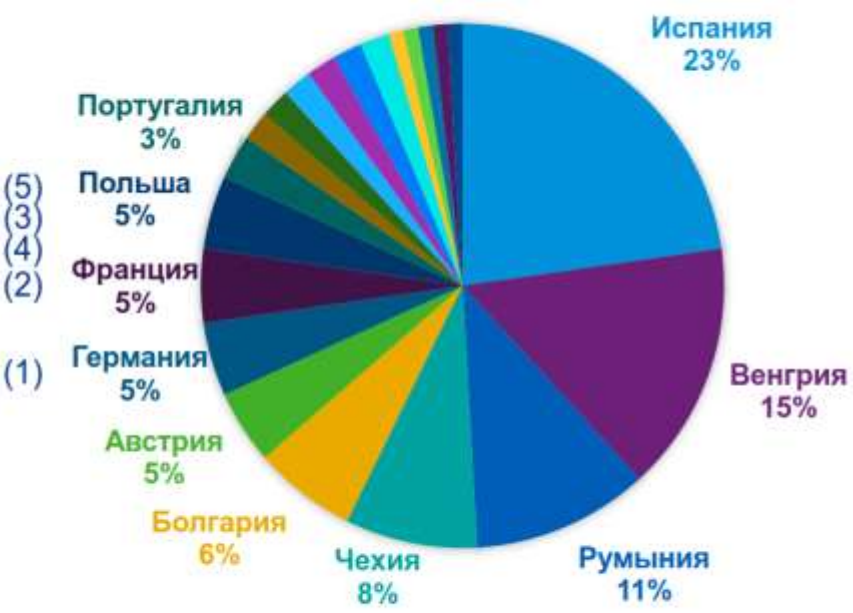
На 8 ноября

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

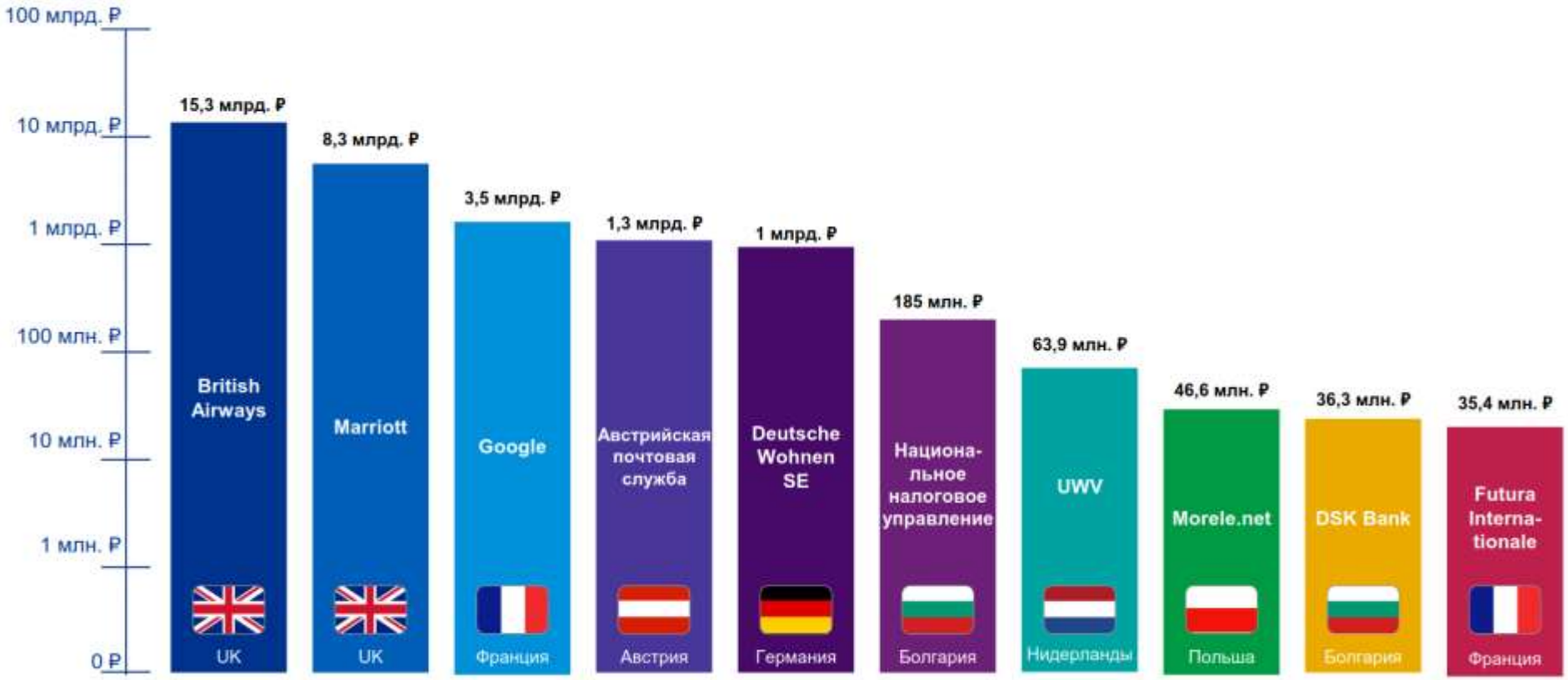
Страна	Штрафы	Общая сумма (₽)
Испания	25	72 378 265
Венгрия	17	12 928 217
Румыния	12	31 567 515
Чехия	9	1 250 001
Болгария	7	223 733 927
Австрия	5	1 281 935 618
Германия	5	1 045 915 403
Франция	5	3 626 720 300
Польша	5	67 001 753
Португалия	3	29 950 606
Великобритания	2	23 518 246 599
Греция	2	39 035 150
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)



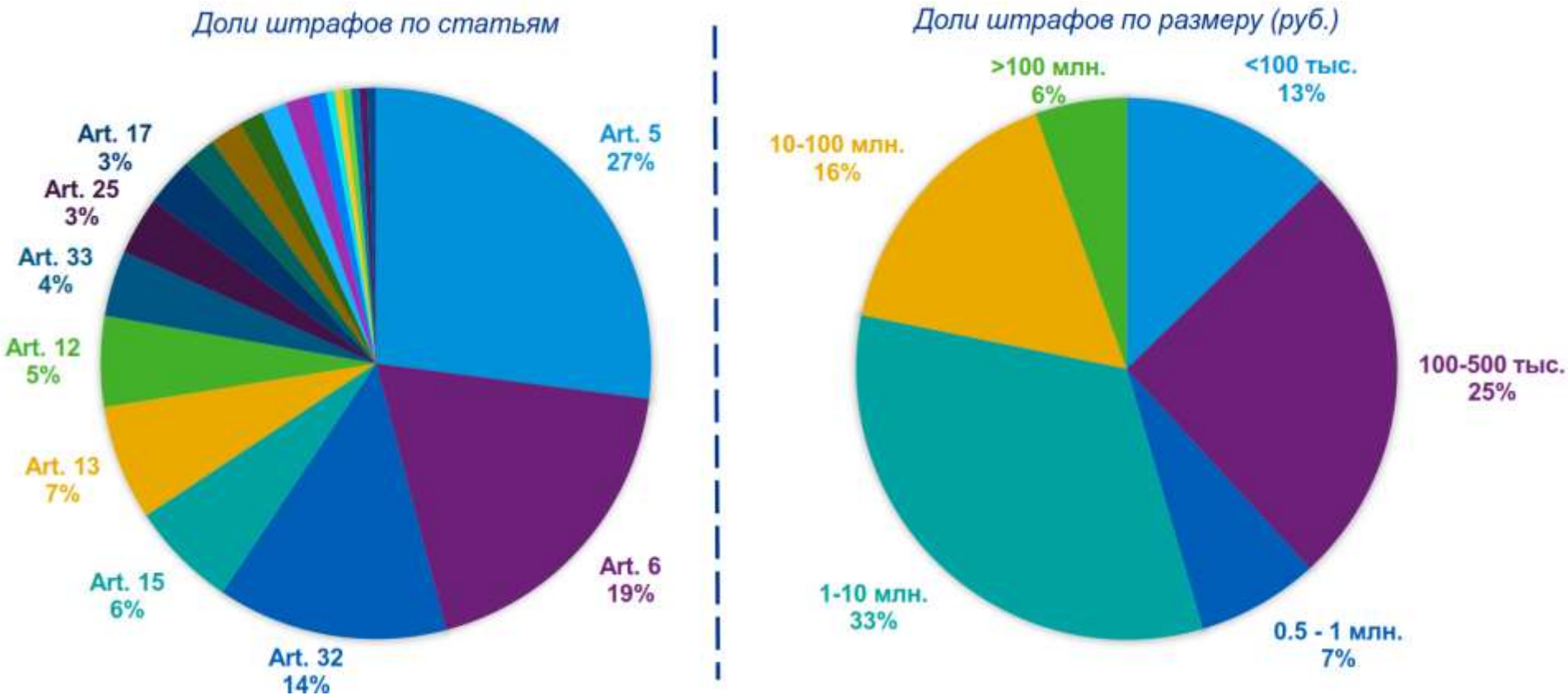
http://rppa.ru/files/2019-12-03_gdpr.pdf

203 Аналитика KPMG по штрафам GDPR на 03.12.2019



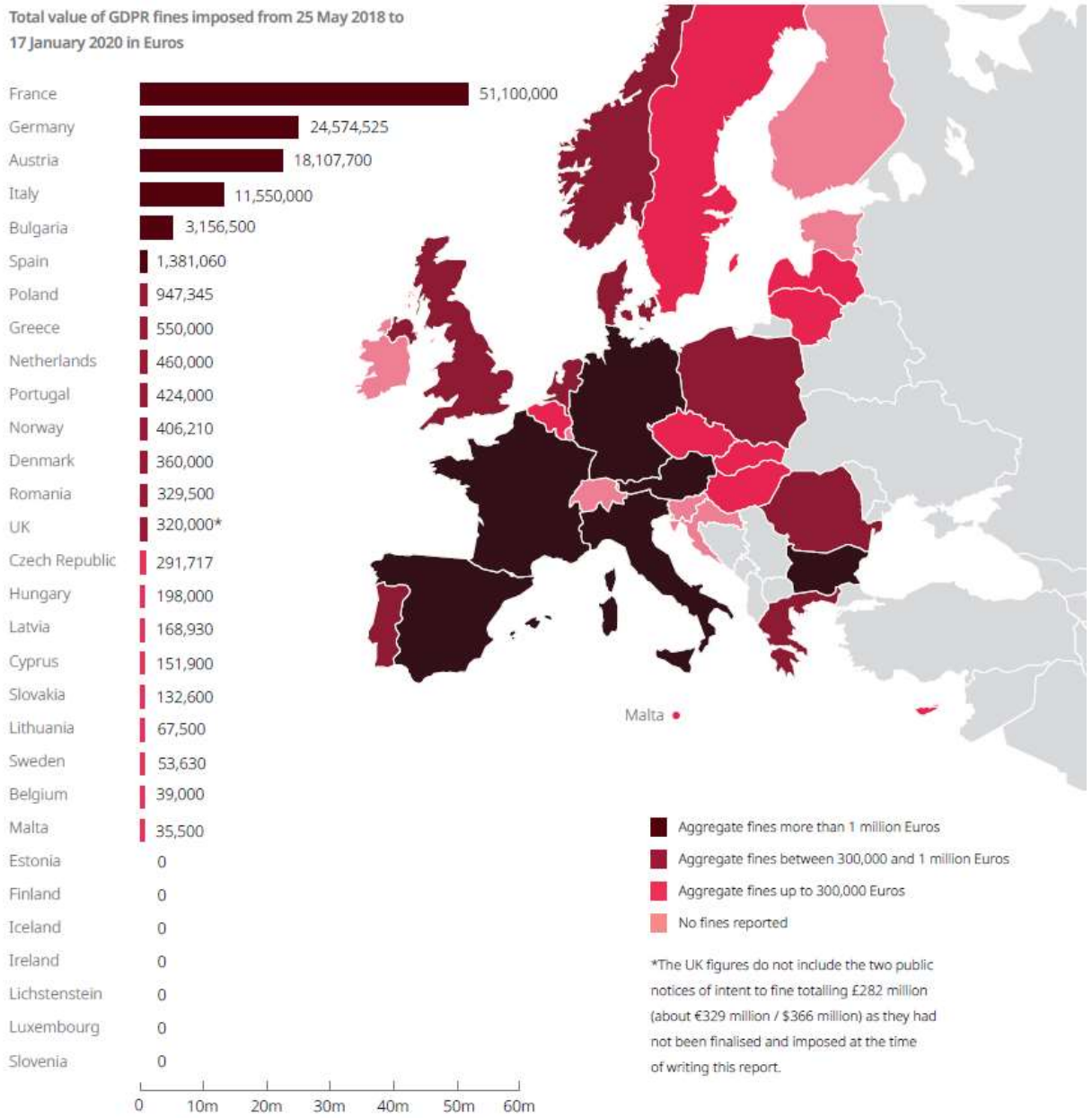
http://rppa.ru/files/2019-12-03_gdpr.pdf

204 Аналитика KPMG по штрафам GDPR на 03.12.2019



http://rppa.ru/files/2019-12-03_gdpr.pdf

205 Статистика штрафов в 2018-2019 годах от DLA Piper



https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/

Разработка методики по расчету и наложению штрафов в Великобритании, Норвегии и Нидерландов (2019.03)



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

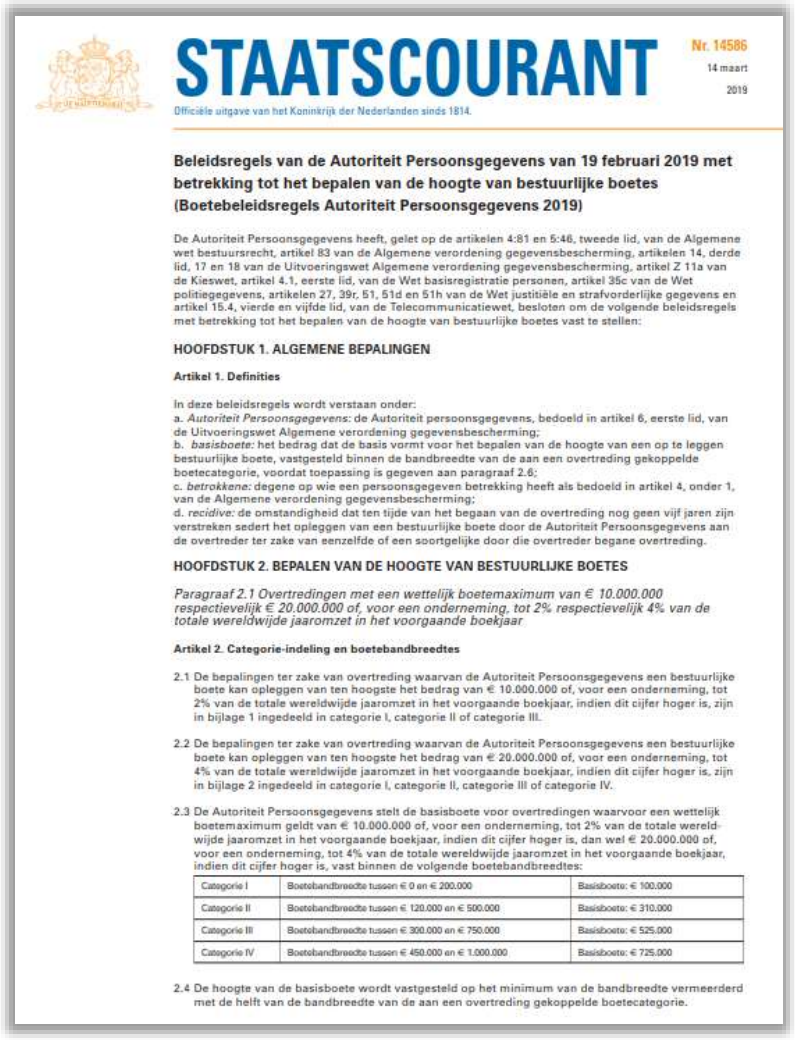
By Rebecca Hill 14 Mar 2019 at 09:56 27 SHARE ▼

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.

https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/

Методика по расчету и наложению штрафов в Нидерландах (2019.05)



STAATSCOURANT

Nr. 14586
14 maart
2019

Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.

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, gelet 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 Z 11a van de Kieswet, artikel 4.1, eerste lid, van de Wet basisregistratie personen, artikel 35c 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 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

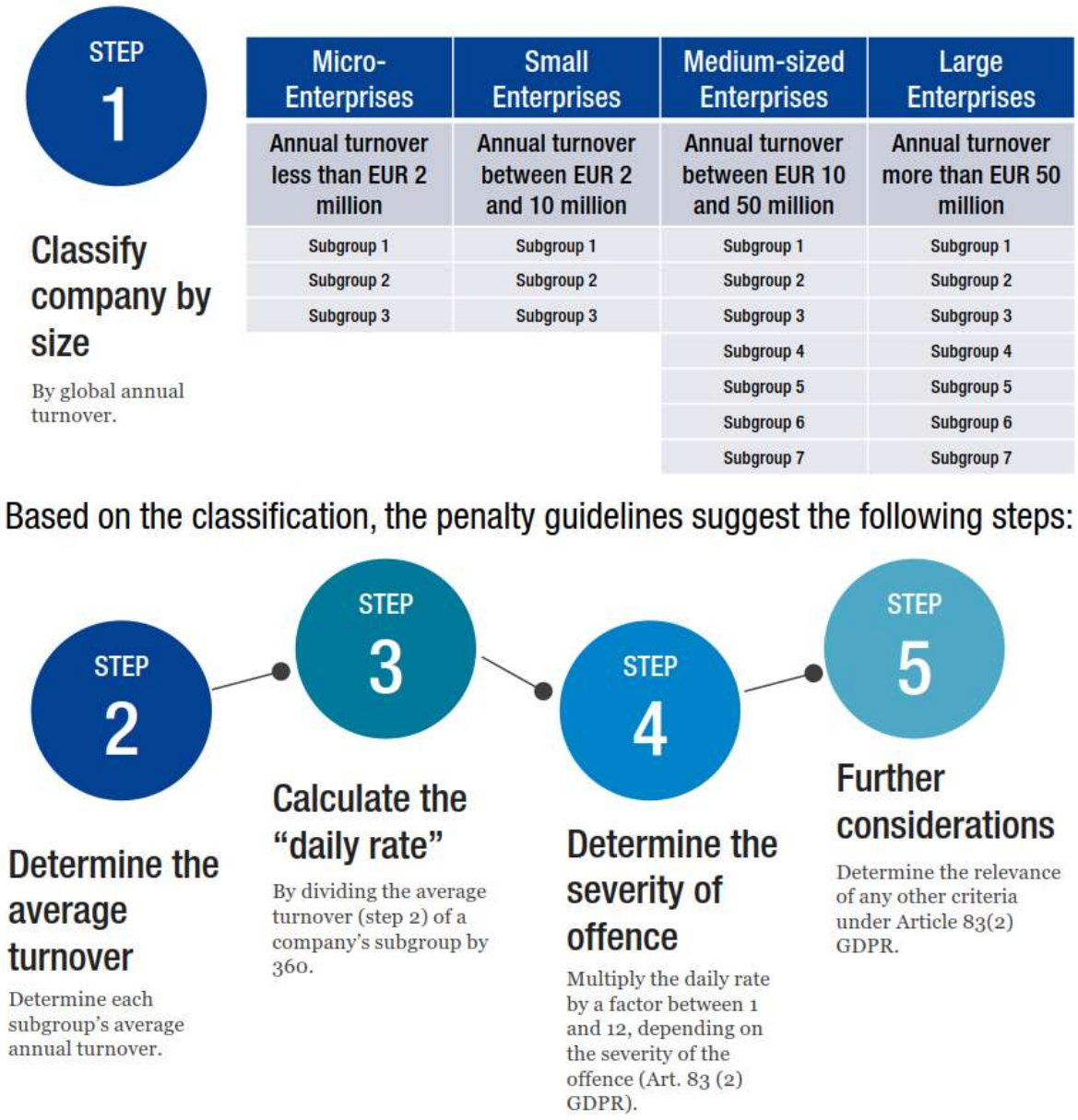
2.4 De hoogte van de basisboete wordt vastgesteld op het minimum van de bandbreedte vermeerderd met de helft van de bandbreedte van de aan een overtreding gekoppelde boetecategorie.

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

Category	Standard fine bandwidth	Standard penalty
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.		

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586.pdf

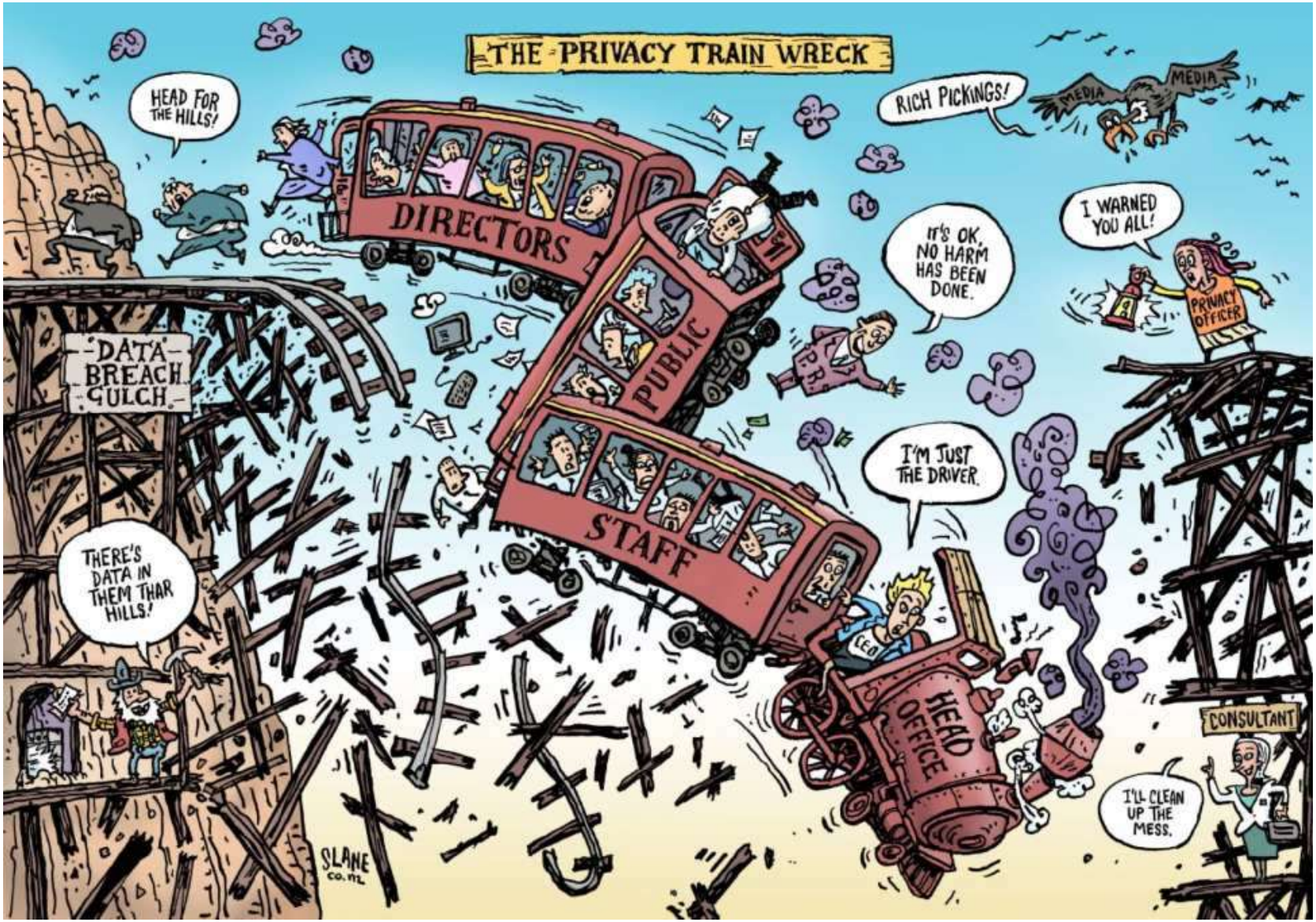
Методика по расчету и наложению штрафов в Германии (2019.10)



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.

https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf

Штрафы - интересные кейсы



К оглавлению

210 Штраф за неразграниченные доступа к данным пациентов



Portuguese Data Protection Authority Imposes 400,000 € Fine on Hospital

The Barreiro Hospital in Portugal was fined 400,000 € by the Portuguese Data Protection Authority CNPD (Comissão Nacional de Proteção de Dados) for incompliancy 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 CNPS 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

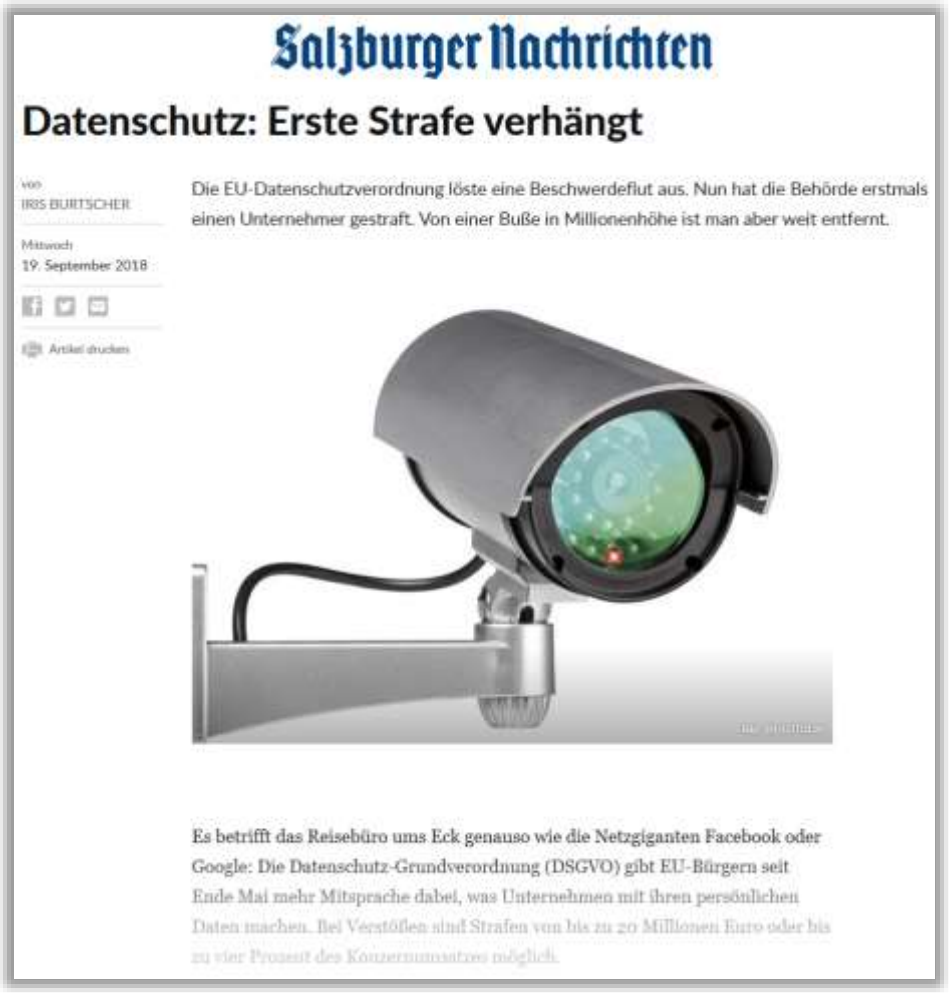
За что: нарушение ст. 5(1)(f) и 32 GDPR

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 права доступа для врачей, в то время как в больнице работают 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).

https://www.datenschutz-notizen.de/portuguese-data-protection-authority-imposes-400000-e-fine-on-hospital-4821441/

211 Штраф за неправильно настроенную систему CCTV



Salzburger Nachrichten

Datenschutz: Erste Strafe verhängt

von
IRIS BURTSCHER

Mittwoch
19. September 2018

Artikel drucken

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.

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.

https://www.derstandard.de/story/2000092017999/erst-vier-strafen-wegen-dsgvo-seit-mai

212 Штраф за отсутствие Controller-to-Processor Agreement



heise online heise+

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 vereinzelte 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.

https://www.heise.de/newsticker/meldung/DSGVO-5000-Euro-Bussgeld-fuer-fehlenden-Auftragsverarbeitungsvertrag-4282737.html

213 Штраф за нарушение законодательства о защите прав потребителей в Италии



AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

Seguici su

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 prospettazione di rilevanti limitazioni alla fruibilità del social network e dei siti web/app di terzi; ciò condizionagli 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

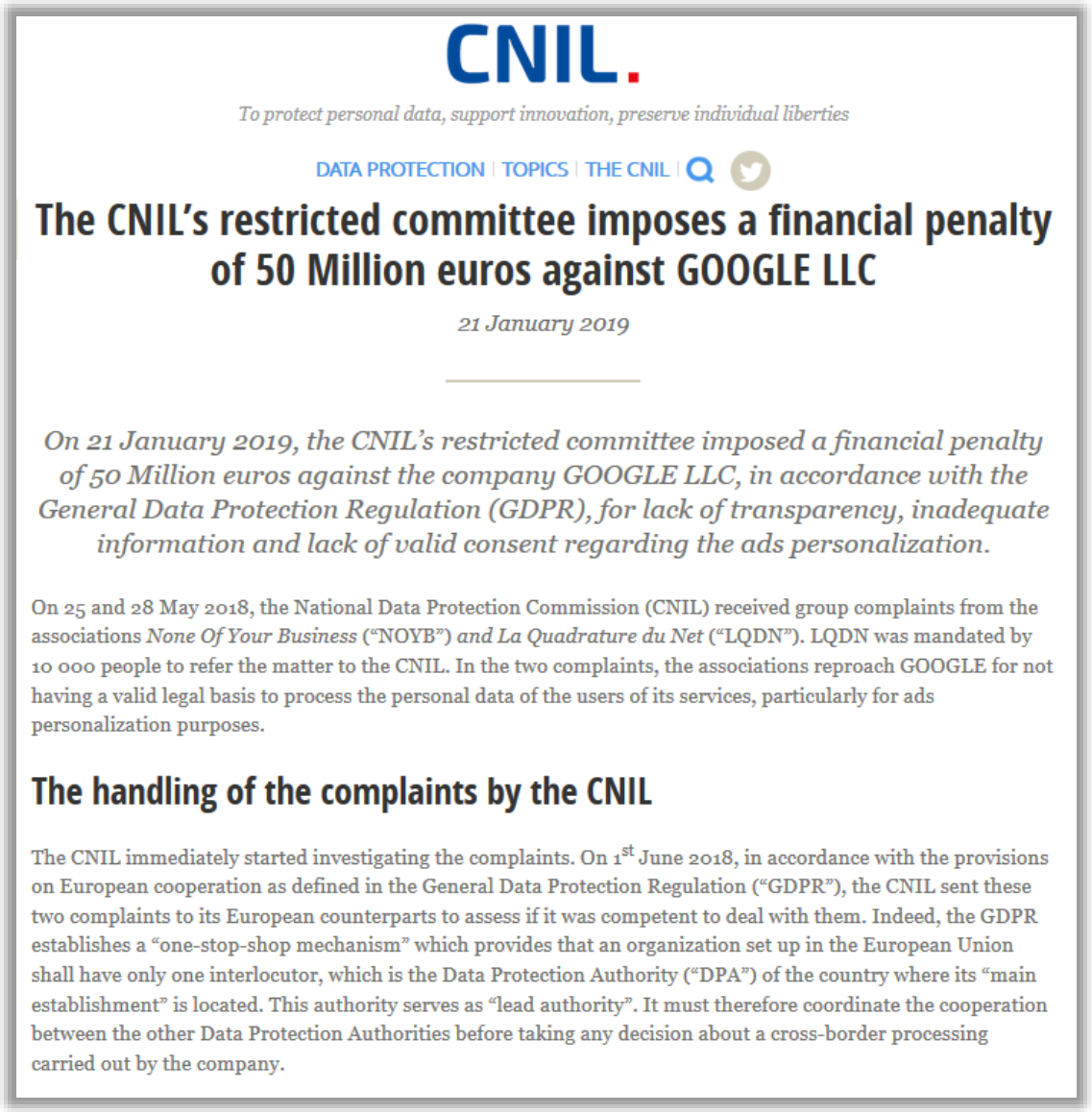
За что: нарушение ст. 21 и 22 Codice del Consumo (Кодекса потребителей)

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.

http://www.agcm.it/media/comunicati-stampa/2018/12/Uso-dei-dati-degli-utenti-a-fini-commerciali-sanzioni-per-10-milioni-di-euro-a-Facebook

214 Штраф за непрозрачность и ненадлежащие согласия



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 Inc.

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.

https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Штраф за нарушение принципа «ограничения целью» (purpose limitation)



Кто: Datatilsynet (Норвегия)

Кого: Tolldirektoratet (Таможенное управление Норвегии)

Когда: 2019.03

За что: нарушение ст. 5(1)(b) GDPR

Как: возможный штраф €90,000

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.

https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/varsel-om-gebyr-til-tolldirektoratet

Штраф за нарушение принципа «минимизации объема данных» (data minimization)



DATATILSYNET

GENERELT OM DATABESKYTTELSE EMNER TILSYN OG AFGØRELSER

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 kundernes 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: Taxa 4x35

Когда: 2019.03

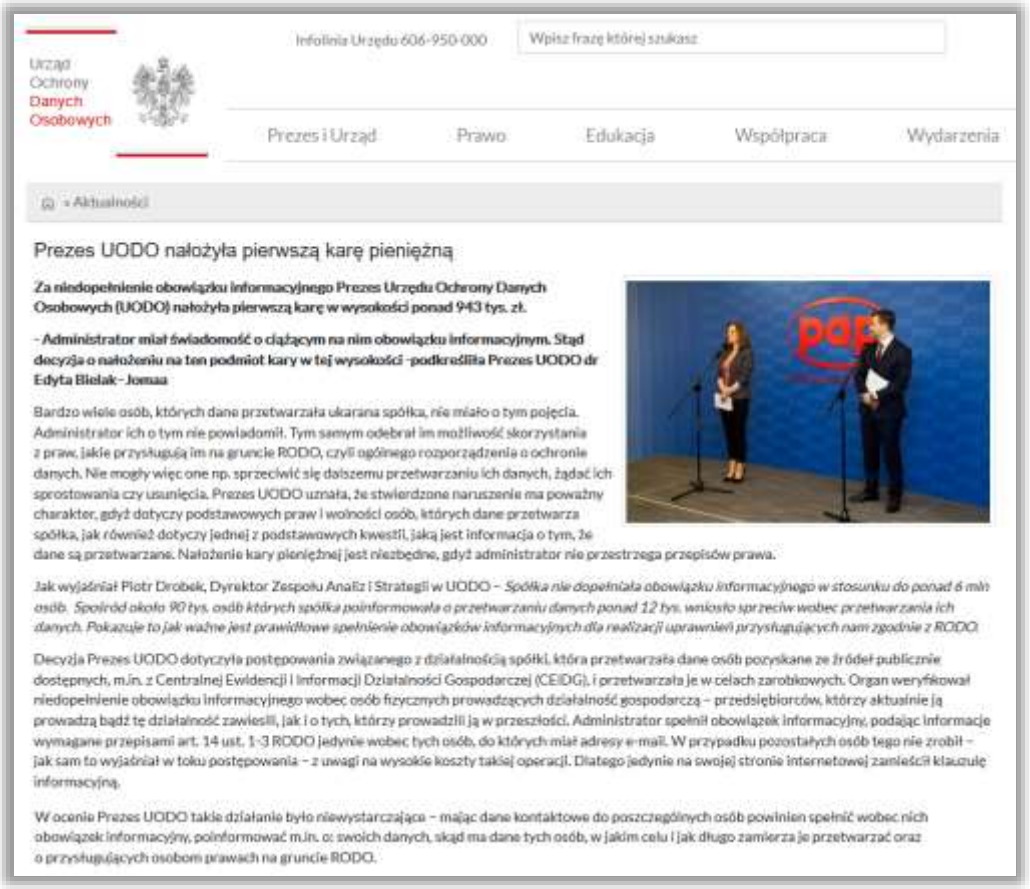
За что: нарушение ст. 5(1)(e) и 6 GDPR

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.

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/mar/tilsyn-med-taxa-4x35s-behandling-af-personoplysninger/

217 Штраф за непредоставление информации при получении персональных данных не от субъекта данных



Urząd Ochrony Danych Osobowych

Infolinia Urzędu 606-950-000 | Wpisz frazę której szukasz

Prezes i Urząd | Prawo | Edukacja | Współpraca | Wydarzenia

» Aktualności

Prezes UODO nałożyła pierwszą karę pieniężną

Za niedopełnienie obowiązku informacyjnego Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożyła pierwszą karę w wysokości ponad 943 tys. zł.

- Administrator miał świadomość o ciążącym na nim obowiązku informacyjnym. Stąd decyzja o nałożeniu na ten podmiot kary w tej wysokości -podkreśliła Prezes UODO dr Edyta Bielak-Jomaa

Bardzo wiele osób, których dane 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/номерами телефонов и посчитала слишком дорогостоящим использование таких каналов коммуникации.

https://uodo.gov.pl/pl/138/786

Штраф за неправомерную обработку персональных данных бывших клиентов



DER TAGESSPIEGEL

Verstöße gegen Datenschutz

23.05.2019, 15:29 Uhr

50.000 Euro Bußgeld gegen Onlinebank N26

Es ist eine der bislang höchsten Strafen wegen Verstößen gegen die Datenschutzgrundverordnung: N26 führte wohl eine „schwarze Liste" mit Daten von Ex-Kunden. VON OLIVER VOSS

Neuer Ärger für den Gründer der N26 Bank, Valentin 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».

https://www.tagesspiegel.de/wirtschaft/verstoesse-gegen-datenschutz-50-000-euro-bussgeld-gegen-onlinebank-n26/24375204.html

Штраф за неправомерную обработку персональных данных в избирательных целях



edpb
European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

First Belgian GDPR fine

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 électoral personnalisé par un mandataire public

L'APD a reçu une plainte concernant l'utilisation par un bourgmestre de données obtenues dans le cadre de l'exécution de sa fonction à des fins de campagne électorale.

Les plaignants étaient entrés en contact avec le bourgmestre de la commune via leur architecte dans le cadre d'une modification de lotissement. L'architecte avait, à cette occasion, contacté le bourgmestre par courrier électronique avec en copie les adresses email des plaignants. La veille des élections communales du 14 octobre 2018, le bourgmestre avait alors utilisé la fonction « Reply » de l'email afin d'envoyer un message électoral aux plaignants.

Les deux parties ont été entendues par la Chambre Contentieuse de l'APD ce 28 Mai 2019. Suite à cette audition, la chambre a conclu qu'une infraction au RGPD avait bien été commise.

Non-respect du principe de finalité en protection des données

Le Règlement général sur la protection des données (RGPD) précise que les données collectées par un responsable de traitement (dans ce cas-ci : les adresses emails obtenues par le bourgmestre) doivent être collectées pour des finalités déterminées et ne 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.

https://edpb.europa.eu/news/national-news/2019/first-belgian-gdpr-fine_en

220 Штраф за нарушение принципа «защита данных на основе продуманных действий» (privacy by design)



Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal

Protecţia Datelor | Data Protection | Protection des Donnees

Informaţii generale | Legislaţie | Procedun | Relaţii Internaţionale | Contact

Home » Comunicat_amenda_Unicredit

8/07/2019 19:04 Română | English | Francais

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

Plângeri

Plângeri RGPD

Procedura de soluţionare

Operatori

Formular declarare responsabil cu protecţia datelor

Notificare Breşă RGPD

Notificare Breşă L.506/2004

Informaţi plată amendă persoane juridice

Informaţii utile

Întrebări frecvente

Ghid întrebări RGPD

Ghid orientativ RGPD

Legături utile

Stiri

08/07/2019

O nouă amendă în aplicarea GDPR

04/07/2019

Prima amendă în aplicarea RGPD

PRIMA AMENDĂ ÎN APLICAREA RGPD

Pe data de 27.06.2019, **Autoritatea Naţională de Supraveghere a finalizat o investigaţie la operatorul UNICREDIT BANK S.A. şi a constatat că acesta a încălcat prevederile art. 25 alin. (1) din Regulamentul (UE) 2016/679** al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).

Operatorul a fost sancţionat contravenţional cu amendă în cuantum de 613.912 lei, echivalentul în euro al sumei de 130.000 euro.

Sancţiunea a fost aplicată UNICREDIT BANK S.A. ca urmare a neaplicării măsurilor tehnice şi organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât şi în cel al prelucrării în sine, destinate să pună în aplicare în mod eficient principiile de protecţie a datelor, precum reducerea la minimum a datelor, şi să integreze garanţiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele RGPD şi a proteja drepturile persoanelor vizate. Aceasta a condus la dezvăluirea în documentele ce conţin detaliile tranzacţiilor şi care sunt puse on-line la dispoziţia clienţilor beneficiari ai plăţilor, a datelor privind CNP-ul şi adresa plătitorului (pentru situaţiile în care plătitorul efectua tranzacţia dintr-un cont deschis la o altă instituţie de credit - tranzacţii externe şi depuneri la casierie), respectiv a datelor privind adresa plătitorului (pentru situaţiile în care plătitorul efectua tranzacţia dintr-un cont deschis la UNICREDIT BANK SA - tranzacţii interne), pentru un număr de 337.042 persoane vizate, în perioada 25 mai 2018 – 10.12.2018.

Sancţiunea a fost aplicată ca urmare a unei sesizări a Autorităţii Naţionale de Supraveghere din data de 22.11.2018 prin care se semnala faptul că datele privind CNP-ul şi adresa persoanelor care efectuau plăţi la UNICREDIT BANK S.A., prin intermediul tranzacţiilor on-line, erau dezvăluite către beneficiarul tranzacţiei, 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 obligaţia de a prelucra date limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate datele.

În acelaşi timp, considerentul (78) din Regulament precizează: "Protecţia drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice şi organizatorice corespunzătoare pentru a se asigura îndeplinirea cerinţelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne şi să pună în aplicare măsuri care să respecte în special principiul protecţiei datelor începând cu momentul conceperii şi cel al protecţiei 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, transparenţa în ceea ce priveşte funcţiile şi prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranţă şi să le îmbunătăţească. Atunci când elaborează, proiectează, selectează şi utilizează aplicaţii, servicii şi produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-şi îndeplini rolul, producătorii acestor produse şi furnizorii acestor servicii şi aplicaţii ar trebui să fie încurajaţi să aibă în vedere dreptul la protecţia datelor la momentul elaborării şi proiectării unor astfel de produse, servicii şi aplicaţii şi, ţinând cont de stadiul actual al dezvoltării, să se asigure că operatorii şi persoanele împuternicite de operatori sunt în măsură să îşi îndeplinească obligaţiile referitoare la protecţia datelor. Principiul protecţiei datelor începând cu momentul conceperii şi cel al protecţiei implicite a datelor ar trebui să fie luate în considerare şi în contextul licitaţiilor publice."

Biroul juridic şi comunicare

A.N.S.P.D.C.P.

Кто: Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Persona (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.

https://www.dataprotection.ro/index.jsp?page=Comunicat_Amenda_Unicredit

Штраф за нарушение принципа «ограничения срока обработки» (storage limitation)



DATATILSYNET

Møbelfirma indstillet til bøde

Publiceret 11-06-2019

Nyhed

Datatilsynet har politianmeldt IDdesign A/S og indstillet virksomheden til en bøde på 1,5 mio kr. for manglende sletning af oplysninger om ca. 385.000 kunder.

I efteråret 2018 var Datatilsynet på tilsynsbesøg hos IDdesign, hvor der bl.a. blev set på, om virksomheden havde fastsat frister for sletning af kundernes oplysninger, og om fristerne blev efterlevet.

Ingen slettefrister

Forud for tilsynsbesøget havde IDdesign sendt en oversigt over de systemer, som virksomheden anvender til behandling af personoplysninger. IDdesign oplyste i den forbindelse, at der i enkelte IDEmøbler-butikker fortsat anvendes et ældre system, som ellers er erstattet af et nyere system i de andre butikker, og at der i det gamle system behandles oplysninger om ca. 385.000 kunders navn, adresse, telefonnummer, e-mail og købshistorik. Under tilsynsbesøget oplyste IDdesign endvidere, at der ikke er fastsat slettefrister i dette system, hvorfor personoplysninger i det gamle system aldrig er blevet slettet.

Derfor indstilles der til bøde

Det fremgår af databeskyttelsesforordningen, at personoplysninger skal opbevares, så det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

Кто: Datatilsynet (Дания)

Кого: мебельная компания IDdesign A/S

Когда: 2019.06

За что: нарушение ст. 5(1)(e) и 5(2) GDPR

Как: штраф €201,000

Причина: в ходе проведенного 08.10.2018 года аудита был выявлен факт использования компанией IDdesign ERP-систем AX 2.5 и AX 2012, для которых не были определены сроки обработки персональных данных около 385,000 клиентов (ФИО, адрес, номер телефона, адрес электронной почты и история покупок) мебельных магазинов IDE, а также не осуществлялось прекращение обработки персональных данных клиентов после достижения цели их обработки. Кроме того, для системы подбора персонала YoungCRM и системы управления персоналом Timetable не были документированы процедуры уничтожения персональных данных.

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/jun/tilsyn-med-iddesigns-behandling-af-personoplysninger/

222 Штраф за неправомерное использование системы видеонаблюдения



МЕДИАТЕКА | 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)(c), 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.

https://www.cnil.fr/fr/uniontrad-company-20-000-euros-damende-pour-videosurveillance-excessive-des-salaries

223 Самый большой штраф за нарушение GDPR



Search jobs | Sign in | Search | The Guardian | International edition

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

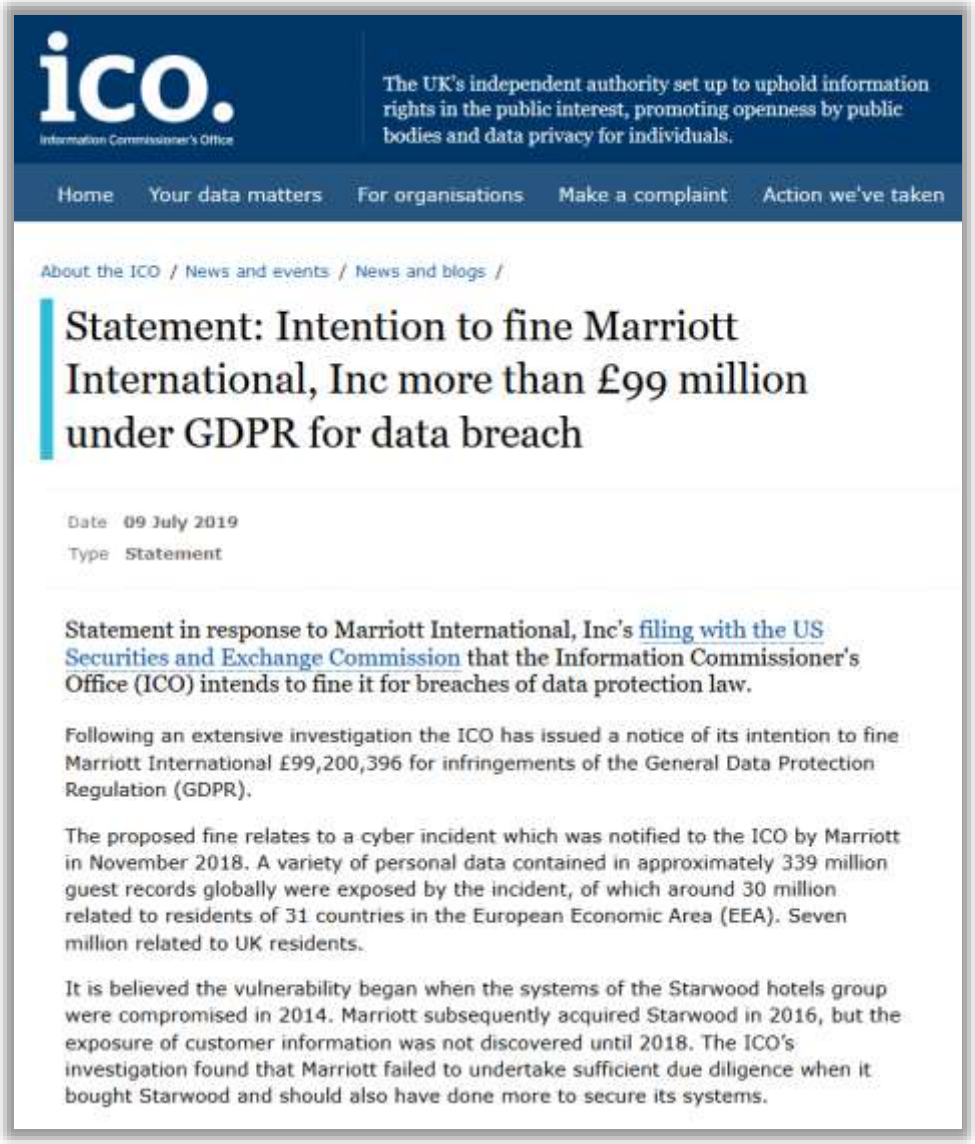
Как: штраф €204,600,000

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: Hight 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.

https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways
https://www.itgovernance.co.uk/blog/british-airways-data-breach-class-action-lawsuit-approved

Штраф за самую большую утечку (339 млн. записей) персональных данных



ico.
Information Commissioner's Office

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

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

About the ICO / News and events / News and blogs /

Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach

Date 09 July 2019
Type Statement

Statement in response to Marriott International, Inc's filing with the US Securities and Exchange Commission that the Information Commissioner's Office (ICO) intends to fine it for breaches of data protection law.

Following an extensive investigation the ICO has issued a notice of its intention to fine Marriott International £99,200,396 for infringements of the General Data Protection Regulation (GDPR).

The proposed fine relates to a cyber incident which was notified to the ICO by Marriott in November 2018. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents.

It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.

Кто: Information Commissioner's Office (Великобритания)

Кого: Marriott International, Inc

Когда: 2019.07

За что: нарушение ст. 32 GDPR

Как: штраф €110,390,200

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.

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

Штраф за необеспечение защиты персональных данных ТВ-звезды



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.

https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-patiëntendossiers

226 Штраф за необеспечение защиты персональных данных 6 млн. лиц



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.

https://www.cpdp.bg/index.php?p=news_view&aid=1519

Штраф за обработку биометрических персональных данных несовершеннолетних



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 → Sanktionsavgift för ansiktsigenkänning i skola

Publicerad 2019-08-21

Sanktionsavgift för ansiktsigenkänning i skola

Datainspektionen utfärdar en sanktionsavgift på 200 000 kronor för en skola som på prov har använt ansiktsigenkänning via kamera för att registrera elevers 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 ansiktsigenkänning via kamera för att registrera elevers 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

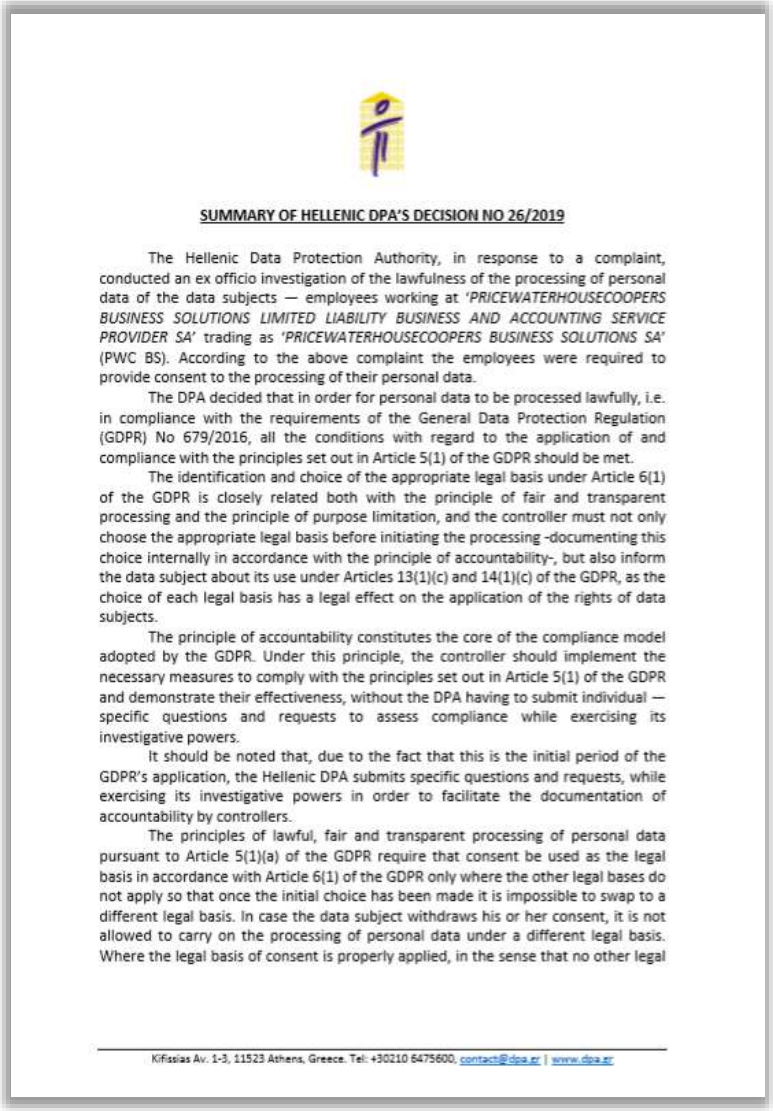
За что: нарушение ст. 5(1)(c), 9, 35, 36 GDPR

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).

https://www.datainspektionen.se/nyheter/sanktionsavgift-for-ansiktsigenkanning-i-skola/

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

Kifissias Av. 1-3, 11523 Athens, Greece. Tel: +30210 6475600, contact@dpa.gr | www.dpa.gr

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.

http://www.dpa.gr/pls/portal/url/ITEM/8EE3F6C3205752BAE050A8C07E241771

Штраф за непредоставление информации при получении персональных данных не от субъекта данных


Urząd Ochrony Danych Osobowych

Wpisz frazę której szukasz

Infolinia Urzędu 606-950-000

Prezes i Urząd | Prawo | Edukacja | Współpraca | Pora

» Aktualności

Kara za niewystarczające zabezpieczenia organizacyjne i techniczne

Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) nałożył na spółkę Morele.net karę w wysokości ponad 2,8 mln zł.

Zastosowane przez spółkę środki organizacyjne i techniczne ochrony danych osobowych nie były odpowiednie do istniejącego ryzyka związanego z ich przetwarzaniem, przez co dane około 2 mln 200 tys. osób dostały się w niepowołane ręce. Zabrakło odpowiednich procedur reagowania na wypadek pojawiania się nietypowego ruchu w sieci – uznał Prezes UODO.

Nakładając karę, organ nadzorczy stwierdził, że naruszenie, do 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 могло быть причиной утечки следующих данных 35,000 субъектов: имя, фамилия, номер телефона, электронная почта, адрес доставки, ID номер, доход и тд.

https://edpb.europa.eu/news/national-news/2019/polish-dpa-imposes-eu645000-fine-insufficient-organisational-and-technical_en

Штраф за нарушение принципа «защита данных на основе продуманных действий» (privacy by design)



edpb

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

Administrative fines imposed on a telephone service provider

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: Архής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Греция)

Кого: Hellenic Telecommunications Organization (OTE)

Когда: 2019.10

За что: нарушение ст. 5(1)(c), 21(3), 25 GDPR

Как: штраф € 400,000

Причина: Клиенты Греческой телефонной компании получали рекламные рассылки без возможности отписки. Также клиенты из do-not-call register получали рекламные звонки от сторонних компаний.

https://edpb.europa.eu/news/national-news/2019/administrative-fines-imposed-telephone-service-provider_en

231 Не только большой штраф, но и компенсация субъекту



edpb
European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

European Data Protection Board › News › National News › National News › Administrative criminal proceedings of the Austrian data protection authority against Österreichische Post AG (Austria

Administrative criminal proceedings of the Austrian data protection authority against Österreichische Post AG (Austrian Postal Service)

Wednesday, 23 October, 2019 AT

The Austrian data protection authority (DPA) imposed an administrative fine of 18 million euros on Österreichische Post AG (ÖPAG) after conducting administrative fine proceedings.

After carrying out an oral hearing, the Austrian DPA considered it established on the basis of the evidence that ÖPAG had violated the GDPR by processing personal data on the alleged political affinity of affected data subjects.

In addition, another violation was determined due to the further processing of data on package frequency and the frequency of relocations for the purpose of direct marketing, as this is not covered by the GDPR.

These violations of the GDPR were committed unlawfully and culpably, which is why the above-mentioned administrative fine is appropriate to prevent other or similar violations.

The penalty is not final, as it can be challenged before the Federal Administrative Court within four weeks after the delivery of the penalty notice.

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

Причина: Почта использовала адрес и возраст субъектов для определения принадлежности к политическим партиям, а полученные предполагаемые данные продавала третьим лицам. Также почта с целью маркетинга анализировала частоту переездов субъектов.

Последствия: Австрийский суд обязал Österreichische Post AG выплатить клиенту компенсацию в €800 (исковое требование было €2,500) за причинённый ущерб ему согласно ст.82 GDPR по причине обработки персональных данных без надлежащего правового основания.

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/

232 Штраф за неразграничение доступа к данным клиентов



Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal

Noi amenzi în aplicarea RGPD

Autoritatea Naţională de Supraveghere a finalizat în data de 01.10.2019 două investigaţii la operatorii **Raiffeisen Bank S.A. şi Vreau Credit S.R.L. constatând următoarele:**

- **Raiffeisen Bank S.A.** a încălcat prevederile **art. 32 alin. (4) coroborat cu art. 32 alin. (1) şi alin. (2) din RGPD**, ceea ce a condus la aplicarea unei amenzi contravenţionale în cuantum de 150.000 Euro
- **Vreau Credit S.R.L.** a încălcat prevederile **art. 32 alin. (4) coroborat cu art. 32 alin. (1) şi alin. (2) din RGPD**, precum şi ale **art. 33 alin. (1) din RGPD**, ceea ce a condus la aplicarea unei amenzi contravenţionale în cuantum de 20.000 Euro.

În ceea ce priveşte **Raiffeisen Bank S.A.**, Autoritatea Naţională de Supraveghere a demarat o investigaţie, ca urmare a transmiterii de către bancă a unei notificări privind încălcarea securităţii datelor cu caracter personal prin completarea formularului privind încălcarea securităţii conform Regulamentului (UE) 2016/679.

Încălcarea securităţii a constat în faptul că doi angajaţi ai Raiffeisen Bank S.A., **utilizând datele din documentele de identitate ale unor persoane fizice**, transmise de către angajaţi ai societăţii Vreau Credit S.R.L. prin intermediul aplicaţiei mobile WhatsApp, **au efectuat interogări ale sistemului Biroului de Credit** pentru a obţine datele necesare în vederea determinării eligibilităţii 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 şi consultarea bazei de date a ANAF.

Simulările de prescoring menţionate mai sus au fost efectuate prin intermediul aplicaţiei informatice utilizate de Raiffeisen Bank S.A. în activitatea de creditare, iar decizia negativă de creditare a fost comunicată de către angajaţii Raiffeisen Bank S.A. către angajaţi Vreau Credit S.R.L., cu încălcarea procedurilor interne.

Sancţiunea a fost aplicată operatorului **ca urmare a faptului că acesta nu a luat măsurile corespunzătoare pentru a se asigura că orice persoană fizică care acţionează sub autoritatea acestuia** şi care are acces la date cu caracter personal, **nu le prelucrează decât la cererea sa**, cu excepţia cazului în care această obligaţie îi revine în temeiul dreptului Uniunii sau al dreptului intern.

De asemenea, operatorul **nu a implementat măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător şi nu a evaluat riscurile pe care le prezintă prelucrarea**.

Această situaţie a condus la **accesul neautorizat la datele cu caracter personal prelucrate** prin aplicaţia informatică utilizată de Raiffeisen Bank S.A. în activitatea de creditare şi **la divulgarea neautorizată** a datelor cu caracter personal de către angajaţi ai băncii.

În ceea ce priveşte operatorul **Vreau Credit S.R.L.**, acesta a fost sancţionat, de asemenea, pentru încălcarea securităţii datelor, dar şi pentru faptul că până la finalizarea investigaţiei nu a notificat autorităţii de supraveghere încălcarea securităţii datelor cu caracter personal, fără întârzieri nejustificate, deşi constatase producerea acestui incident de securitate încă din luna decembrie 2018, ceea ce a condus la încălcarea confidenţialităţii datelor cu caracter personal ale clienţilor proprii (persoanele vizate) şi la prelucrarea neautorizată/ilegală a datelor cu caracter personal ale acestora.

Direcţia juridică şi comunicare

A.N.S.P.D.C.P.

Кто: Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Persona (Румыния)

Кого: Raiffeisen Bank SA

Когда: 2019.10

За что: нарушение 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.

https://www.dataprotection.ro/?page=Comunicat_Presa_09_10_2019

233 Штраф за ненадлежащее ведение RoPA и не только



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, 31 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. n. 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

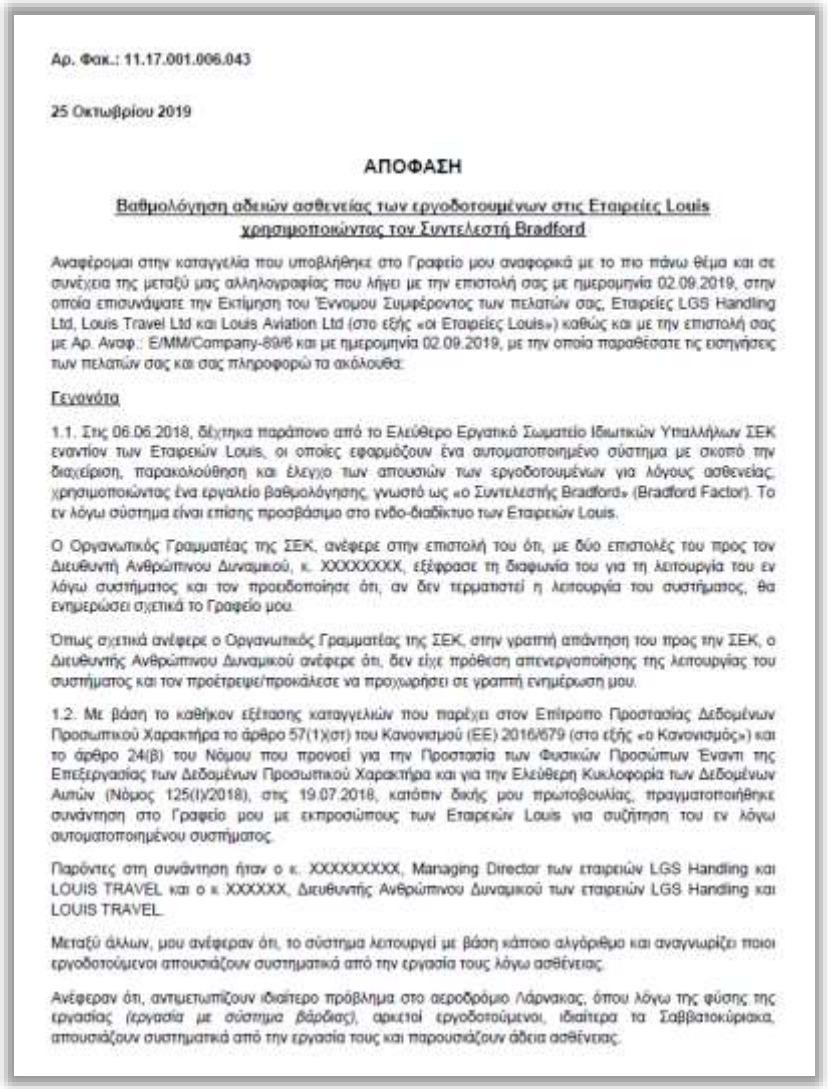
За что: нарушение ст. 5(1)(a), 5(1)(f), 5(1)(e), 5(2), 28(3) GDPR

Как: штраф €9,500 и предписание об устранении нарушений за 60 дней

Причина: Мэр города не заключил Personal 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.

https://edpb.europa.eu/news/national-news/2019/polish-supervisory-authority-imposed-first-administrative-fine-public-entity_en

234 Штраф за некорректный LIA



Αρ. Φακ.: 11.17.001.006.043

25 Οκτωβρίου 2019

ΑΠΟΦΑΣΗ

Βαθμολόγηση αδειών ασθενείας των εργοδοτουμένων 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.: E/MM/Company-89/6 και με ημερομηνία 02.09.2019, με την οποία παραθέσατε τις εισηγήσεις των πελατών σας και σας πληροφορώ τα ακόλουθα:

Γεγονότα

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 εργοδοτουμένων για λόγους ασθενείας, 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 διαφωνία 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 ενημέρωση 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(I)/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. XXXXXXXXX, 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 απουσιάζουν συστηματικά από την εργασία τους λόγω ασθένειας.

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 ασθένειας.

Кто: Графейо Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα (Республика Кипр)

Кого: LGS Handling Ltd, Louis Travel Ltd and Louis Aviation Ltd (Louis Group of Companies)

Когда: 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.

https://edpb.europa.eu/news/national-news/2020/cypriot-supervisory-authority-banned-processing-automated-tool-used-scoring_en

Штраф за нарушение принципа «ограничения целью» (purpose limitation)



edpb

HOME ABOUT EDPB NEWS OUR WORK & TOOLS SEARCH

The Norwegian Data Protection Authority imposes a fine on the Municipality of Oslo, the Education Agency

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 могу 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.

https://edpb.europa.eu/news/national-news/2019/norwegian-data-protection-authority-imposes-fine-municipality-oslo-education_en

Штраф за ненадлежащий механизм отзыва согласия на обработку персональных данных



edpb
European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

Polish DPA: Withdrawal of consent shall not be impeded

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 ПДн субъектов, отказавшихся от обработки их данных и не являющихся клиентами компании, без правового основания.

https://edpb.europa.eu/news/national-news/2019/polish-dpa-withdrawal-consent-shall-not-be-impeded_en

Штраф за неправомерное хранение и несоблюдение сроков хранения персональных данных



Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Pressemitteilung

711.412.1

5. November 2019

Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft

Am 30. Oktober 2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) erlassen.

Bei Vor-Ort-Prüfungen im Juni 2017 und im März 2019 hat die Aufsichtsbehörde festgestellt, dass das Unternehmen für die Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendete, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen. Personenbezogene Daten von Mieterinnen und Mietern wurden gespeichert, ohne zu überprüfen, ob eine Speicherung zulässig oder überhaupt erforderlich ist. In begutachteten Einzelfällen konnten daher teilweise Jahre alte private Angaben betroffener Mieterinnen und Mieter eingesehen werden, ohne dass diese noch dem Zweck ihrer ursprünglichen Erhebung dienten. Es handelte sich dabei um Daten zu den persönlichen und finanziellen Verhältnissen der Mieterinnen und Mieter, wie z. B. Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge.

Nachdem die Berliner Datenschutzbeauftragte im ersten Prüftermin 2017 die dringende Empfehlung ausgesprochen hatte, das Archivsystem umzustellen, konnte das Unternehmen auch im März 2019, mehr als 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
10969 Berlin

Tel: 030 13889 - 900
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, из архива невозможно было удалить данные. Персональные данные (финансовая информация, информация о социальном страховании) хранились без надлежащего правового основания.

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf

Расследование EDPS в отношении Европейского парламента за использование сервисов NationBuilder



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Home | About | Data Protection | Press & Publications

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 голосовании 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.

https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-european-parliaments-2019_en

Штраф за нарушение законодательства о защите прав потребителей в Венгрии



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-модели Facebook заключается в привлечении пользователей контентом своей онлайн-платформы и собре 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.

https://www.gvh.hu/en/press_room/press_releases/press_releases_2019/gvh-imposed-a-fine-of-eur-3.6-m-on-facebook

240 Штраф за ненадлежащую процедуру идентификации



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.

https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverhängtGeldbuße1u1.html

241 Штраф за ненадлежащее хранение 500,000 документов



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

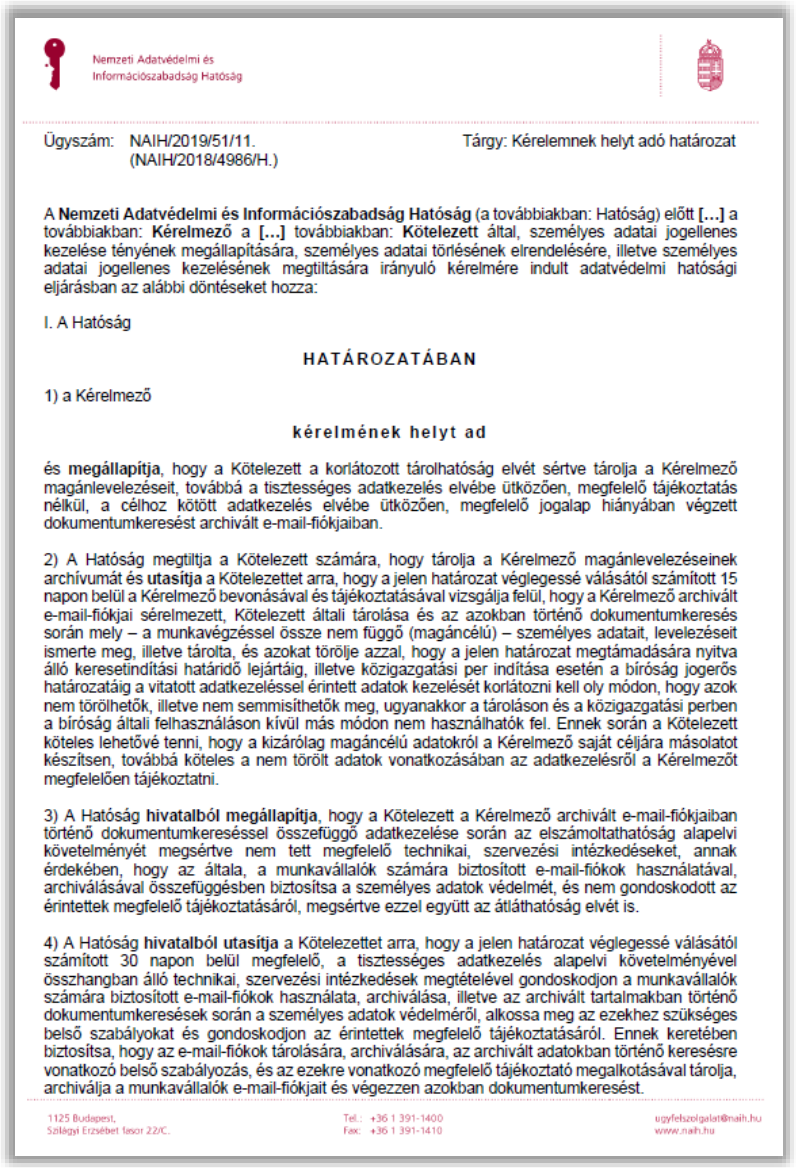
За что: нарушение ст. 5 GDPR

Как: штраф €323,000

Причина: в открытых контейнерах на улице хранились 500,000 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).

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/12/london-pharmacy-fined-after-careless-storage-of-patient-data/

242 Штраф за использование архива корпоративной электронной почты



Nemzeti Adatvédelmi és Információszabadság Hatóság

Ügyszám: NAIH/2019/51/11. (NAIH/2018/4986/H.)

Tárgy: Kérelemnek 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-fiókjaiban.

2) A Hatóság megtiltja a Kötelezett számára, hogy tárolja a Kérelmező magánlevelezéseinek archívumát 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 (magáncélú) – 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 magáncélú 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-fiókjaiban történő dokumentumkereséssel összefüggő adatkezelése során az elszámoltathatóság alapelvi követelményét megsértve 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, megsértve 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 használata, archiválása, 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, Szilágyi Erzsébet fasor 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

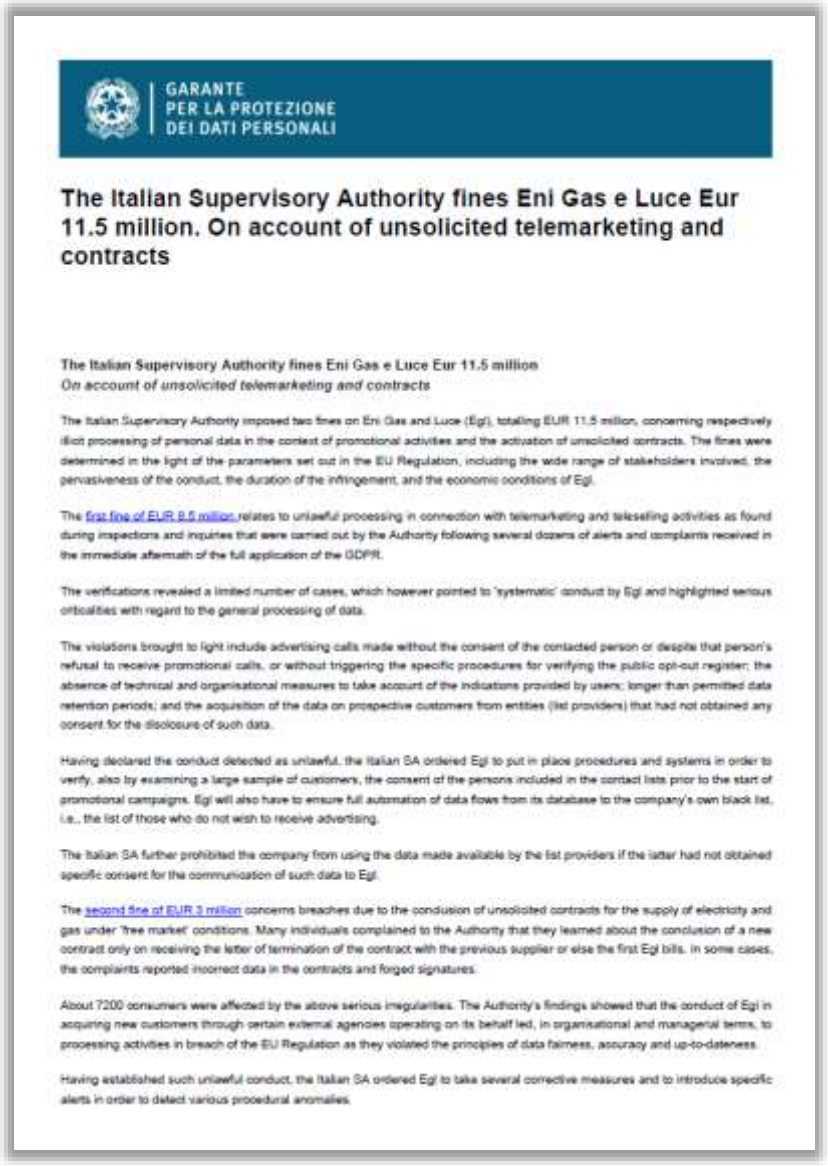
За что: нарушение ст. 5, 6 GDPR

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.

https://www.naih.hu/files/NAIH-2019-51-hatarozat.pdf

Штраф за незаконный прямой маркетинг и навязывание контрактов на поставку продукции



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 (EgI), 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 EgI.

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 EgI 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 EgI 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. EgI 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 EgI.

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 EgI 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 EgI 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 EgI 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. Также 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.

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9245041

Штраф за незаконный прямой маркетинг и нарушение принципа accountability



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Marketing: dal Garante privacy sanzione di 27 milioni e 800 mila euro a Tim

Marketing: dal Garante privacy sanzione di 27 milioni e 800 mila euro a Tim

Il Garante per la privacy ha irrogato a Tim spa una sanzione di 27.802.946 euro per numerosi trattamenti illeciti di dati legati all'attività di marketing. Le violazioni hanno interessato nel complesso alcuni milioni di persone.

Dal gennaio 2017 ai primi mesi del 2019, sono pervenute all'Autorità centinaia di segnalazioni relative, in particolare, alla ricezione di chiamate promozionali indesiderate effettuate senza consenso o nonostante l'iscrizione delle utenze telefoniche nel Registro pubblico delle opposizioni, oppure ancora malgrado il fatto che le persone contattate avessero espresso alla società la volontà di non ricevere telefonate promozionali. Irregolarità nel trattamento dei dati venivano lamentate anche nell'ambito dell'offerta di concorsi a premi e nella modulistica sottoposta agli utenti da Tim.

Dalla complessa attività istruttoria che ne è derivata, svolta anche con il contributo del Nucleo Speciale Tutela Privacy e Frodi 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 Personal" 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).

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9256409

Штраф физическому лицу за незаконный обмен интимными фото и копиями переписки



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.

https://www-euroweeklynews-com.cdn.ampproject.org/c/s/www.euroweeklynews.com/2020/02/06/landmark-penalty-in-spain-as-data-protection-agency-fines-man-e10000-for-sharing-intimate-photos-on-whatsapp/amp/

Штраф Facebook за неназначение DPO и неуведомление надзорного органа



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 EU51,000 penalty
- EU's new privacy rules give authorities higher fining powers

LISTEN TO ARTICLE
▶ 2:00

SHARE THIS ARTICLE
Share
Tweet
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. На размер штрафа положительно повиляла немедленная реакция Facebook на предписание и оперативное предоставление контактных данных DPO.

https://www.bloomberg.com/news/articles/2020-02-13/facebook-fined-in-germany-for-violating-data-protection-rules

247 Штраф за необоснованное полагание на законный интерес



AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Per koerier
KNLTB
[VERTROUWELIJK]
Displayweg 4
3821 BT AMERSFOORT

Datum
20 december 2019

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]
070 8888 500

Onderwerp
Besluit tot het opleggen van een bestuurlijke boete

Geachte [VERTROUWELIJK],

De Autoriteit Persoonsgegevens (AP) heeft besloten aan de vereniging Koninklijke Nederlandse Lawn Tennisbond (KNLTB) een bestuurlijke boete van **€ 525.000,--** op te leggen, omdat de KNLTB in juni en juli 2018 ten behoeve van het genereren van inkomsten een bestand met persoonsgegevens van zijn leden heeft verstrekt aan twee sponsors ten behoeve van direct marketingactiviteiten van deze sponsors. Voor zover het de verstrekking en het gebruik betreft van persoonsgegevens van leden die vóór 2007 lid zijn geworden van de KNLTB, geldt dat dit een onverenigbare verdere verwerking is. Daarmee heeft de KNLTB artikel 5, eerste lid, aanhef en onder b, van de AVG overtreden. Voor zover het de verstrekking en gebruik betreft van persoonsgegevens van leden die ná 2007 lid geworden van de KNLTB, geldt dat daarvoor geen rechtmatige grondslag bestond. Daarmee heeft de KNLTB artikel 5, eerste lid, aanhef en onder a jo. artikel 6, eerste lid, van de AVG overtreden.

Hierna wordt het besluit nader toegelicht. Hoofdstuk 1 betreft een inleiding en hoofdstuk 2 beschrijft het wettelijk kader. In hoofdstuk 3 worden de belangrijkste feiten in deze zaak op een rij gezet. In hoofdstuk 4 beoordeelt de AP de feiten op grond van het wettelijk kader en wordt geconcludeerd dat de KNLTB de AVG heeft overtreden. In hoofdstuk 5 wordt de hoogte van de bestuurlijke boete gemotiveerd. Tenslotte bevat hoofdstuk 6 het dictum en de rechtsmiddelenclausule.

Кто: Autoriteit Persoonsgegevens (Нидерланды)

Кого: Теннисная ассоциация KNLTB

Когда: 2020.03

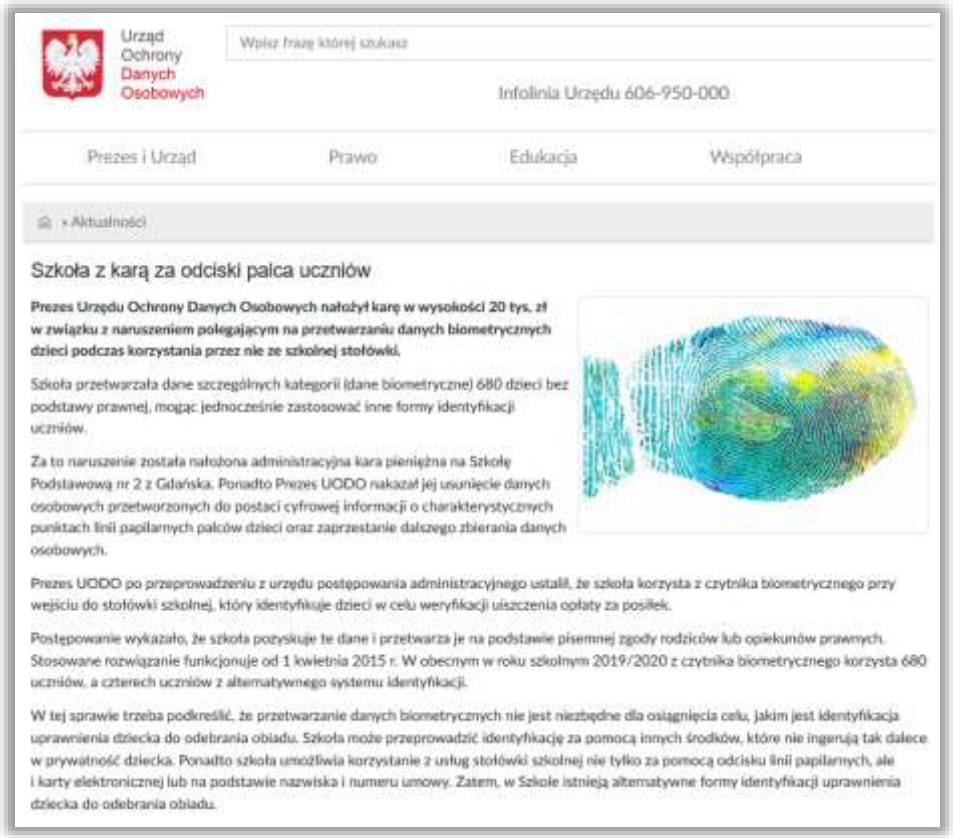
За что: нарушение ст. 5, 6 GDPR

Как: штраф €525,000

Причина: контроллер передал контактные данные нескольких тысяч участников ассоциации спонсорам, которые потом установили прямой контакт с субъектами. Контроллер считал, что передаёт данные на основании своего законного интереса.

https://edpb.europa.eu/news/national-news/2020/dutch-dpa-fines-tennis-association_en

Штраф за безальтернативную биометрическую идентификацию в школе



Urząd Ochrony Danych Osobowych

Wpisz frazę której szukasz

Infolinia Urzędu 606-950-000

Prezes i Urząd | Prawo | Edukacja | Współpraca

» Aktualności

Szkoła z karą za odciski palca uczniów

Prezes Urzędu Ochrony Danych Osobowych nałożył karę w wysokości 20 tys. zł w związku z naruszeniem polegającym na przetwarzaniu danych biometrycznych dzieci podczas korzystania przez nie ze szkolnej stołówki.

Szkoła przetwarzała dane szczególnych kategorii (dane biometryczne) 680 dzieci bez podstawy prawnej, mogąc jednocześnie zastosować inne formy identyfikacji uczniów.

Za to naruszenie została nałożona administracyjna kara pieniężna na Szkołę Podstawową nr 2 z 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 obiadu. Szkoła może przeprowadzić identyfikację za pomocą innych środków, które nie ingerują tak dalece w prywatność dziecka. Ponadto szkoła umożliwia 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 obiadu.

Кто: Urząd Ochrony Danych Osobowych (Польша)

Кого: школа

Когда: 2020.03

За что: нарушение ст. 5, 9 GDPR

Как: штраф €4,400

Причина: контроллер обрабатывал биометрические данных (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.

https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en

Штраф за нарушение со стороны Google права субъекта на забвение (right to be forgotten)



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.

https://www.datainspektionen.se/nyheter/datainspektionen-utfardar-sanktionsavgift-mot-google/

250 Штраф за воспрепятствование проведению проверки



edpb

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

Fine imposed for preventing the Supervisory Authority from performing an inspection

The President of the Personal Data Protection Office imposed a fine of PLN 20 000 on Vis Consulting Sp. z o.o. in liquidation with the seat in Katowice, a company from telemarketing industry, for making it impossible to conduct inspection. Additionally, the company's owner is subject to criminal liability for this.

The President of the Personal Data Protection Office (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 контроллера

Причина: контроллер 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 контроллера. Ещё дважды регулятор безуспешно пытался выйти на контакт с контроллером. Владельцы этой компании решили ее ликвидировать. В соответствии со ст.108(1) 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.

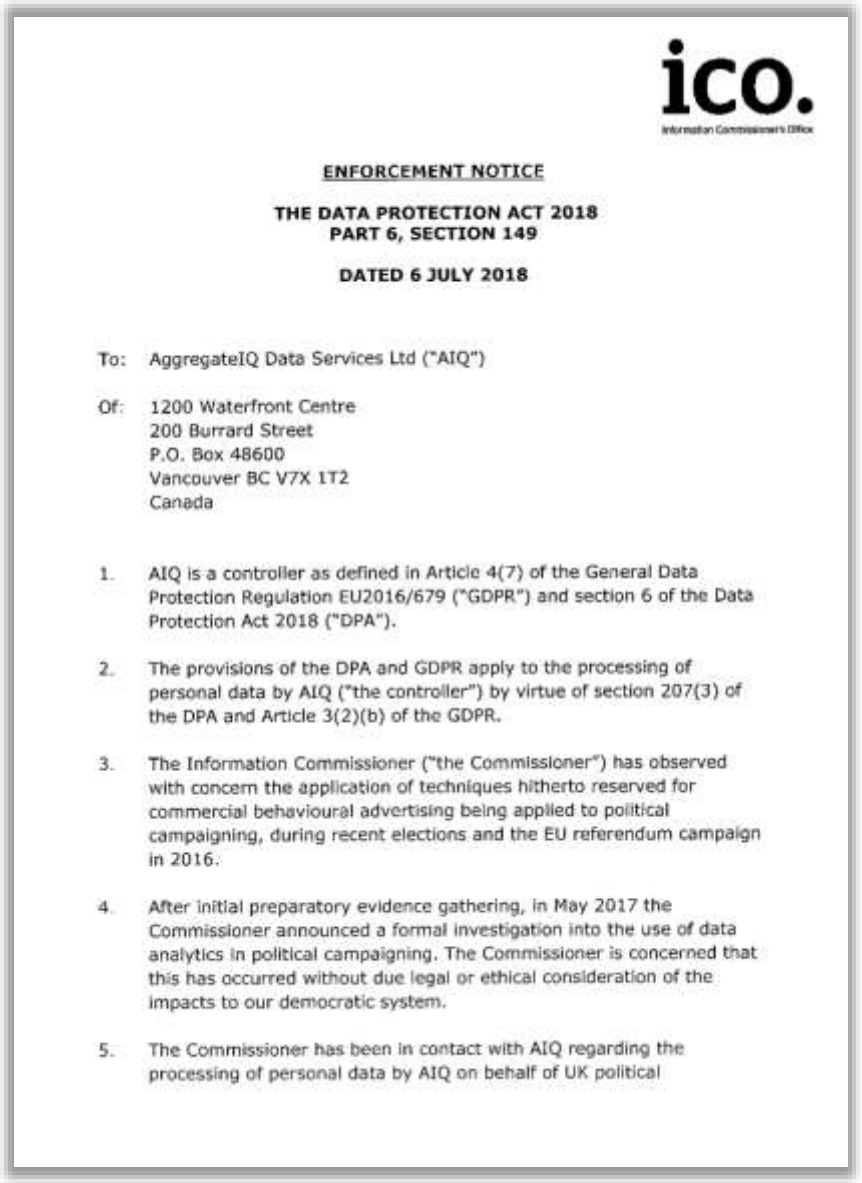
https://edpb.europa.eu/news/national-news/2020/fine-imposed-preventing-supervisory-authority-performing-inspection_en

Иные санкции и меры принуждения



К оглавлению

252 Предписание о прекращении обработки данных



ico.
Information Commissioner's Office

ENFORCEMENT NOTICE

THE DATA PROTECTION ACT 2018
PART 6, SECTION 149

DATED 6 JULY 2018

To: AggregateIQ Data Services Ltd ("AIQ")

Of: 1200 Waterfront Centre
200 Burrard Street
P.O. Box 48600
Vancouver BC V7X 1T2
Canada

1. AIQ is a controller as defined in Article 4(7) of the General Data Protection Regulation EU2016/679 ("GDPR") and section 6 of the Data Protection Act 2018 ("DPA").

2. The provisions of the DPA and GDPR apply to the processing of personal data by AIQ ("the controller") by virtue of section 207(3) of the DPA and Article 3(2)(b) of the GDPR.

3. The Information Commissioner ("the Commissioner") has observed with concern the application of techniques hitherto reserved for commercial behavioural advertising being applied to political campaigning, during recent elections and the EU referendum campaign in 2016.

4. After initial preparatory evidence gathering, in May 2017 the Commissioner announced a formal investigation into the use of data analytics in political campaigning. The Commissioner is concerned that this has occurred without due legal or ethical consideration of the impacts to our democratic system.

5. The Commissioner has been in contact with AIQ regarding the processing of personal data by AIQ on behalf of UK political

Enforcement Notice
of the Information Commissioner,
served under section 149 of DPA18,
on AggregateIQ Data Services Ltd
6 July 2018

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

https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf

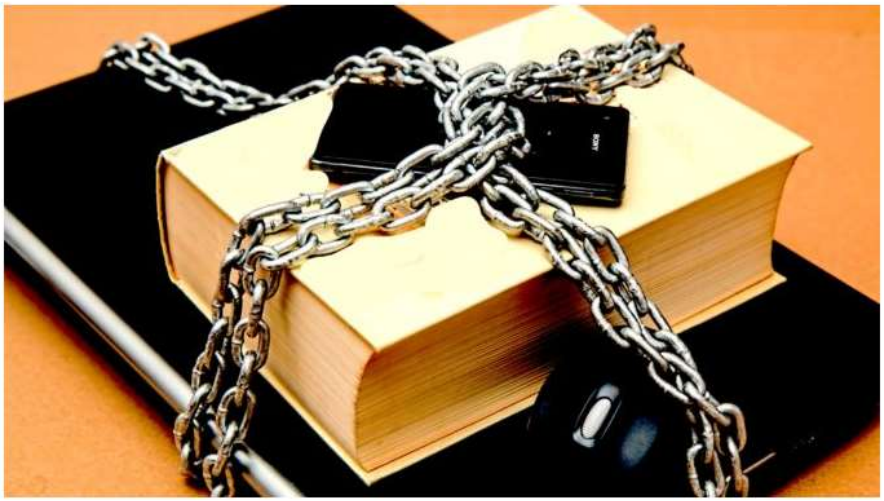
Франция запрещает публикацию судебной аналитики, полученную в том числе с использованием технологий ИИ

ARTIFICIAL LAWYER

CHANGING THE BUSINESS OF LAW

France Bans Judge Analytics, 5 Years In Prison For Rule Breakers

4th June 2019 artificiallawyer Litigation Prediction 36



In a startling intervention that seeks to limit the emerging litigation analytics and prediction sector, the French Government has banned the publication of statistical information about judges' decisions – with a five year prison sentence set as the maximum punishment for anyone who breaks the new law.

Owners of legal tech companies focused on litigation analytics are the most likely to suffer from this new measure.

The new law, encoded in Article 33 of the Justice Reform Act, is aimed at preventing anyone – but especially legal tech companies focused on litigation prediction and analytics – from publicly revealing the pattern of judges' behaviour in relation to court decisions.

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 искусственным интеллектом для анализа судебных решений и построения на его основе достоверных предиктивных моделей, французские судьи решили бороться с этим явлением.

https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers/

Предписание об изменении процесса обработки персональных данных



edpb
European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

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

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.

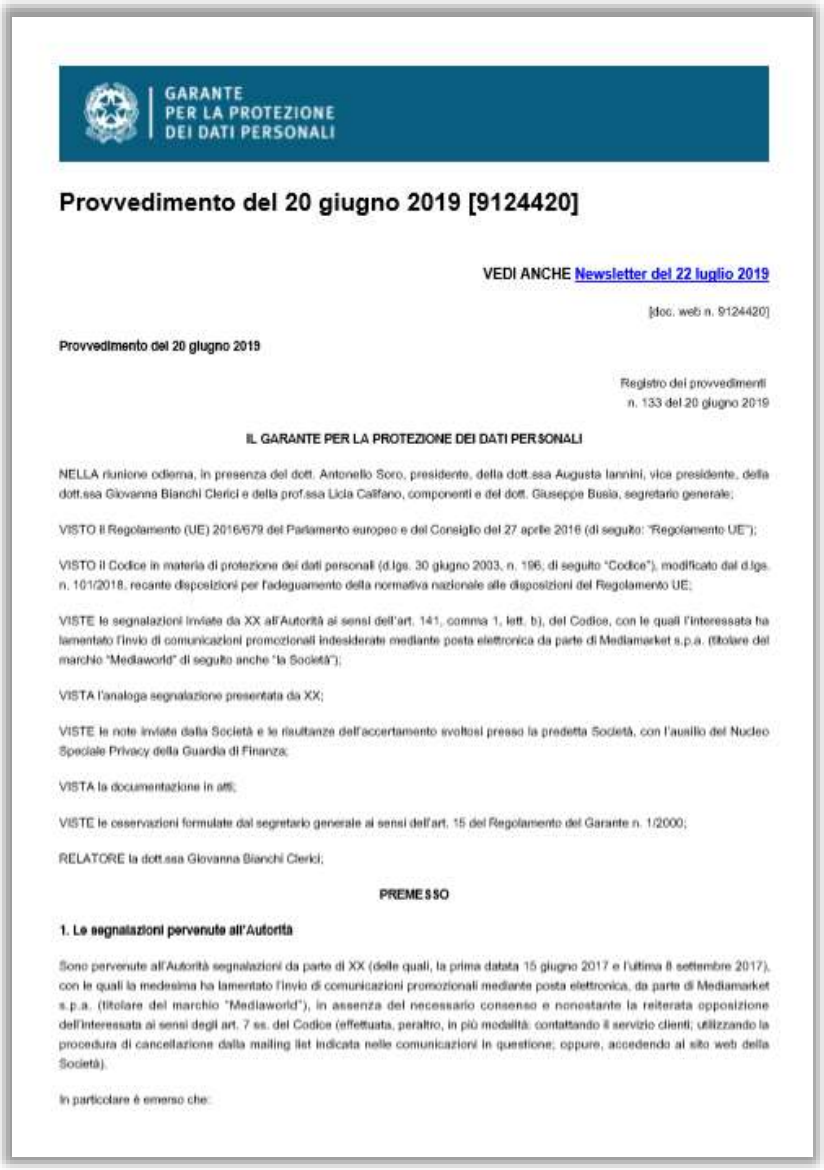
Further information:
Data Protection Ombudsman Reijo Aarnio, tel. +358 40 520 7068, reijo.aarnio(at)om.fi

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.

https://edpb.europa.eu/news/national-news/2019/data-protection-ombudsman-ordered-svea-ekonomi-correct-its-practices_en

255 Угроза лишения свободы от GPDP



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento del 20 giugno 2019 [9124420]

VEDI ANCHE Newsletter del 22 luglio 2019

[doc. web n. 9124420]

Provvedimento del 20 giugno 2019

Registro dei provvedimenti
n. 133 del 20 giugno 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito: "Regolamento UE");

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 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 8 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:

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.

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124420

Зальцбургский адвокат судится против ряда онлайн-сервсиов на основании ст.82 GDPR



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.).

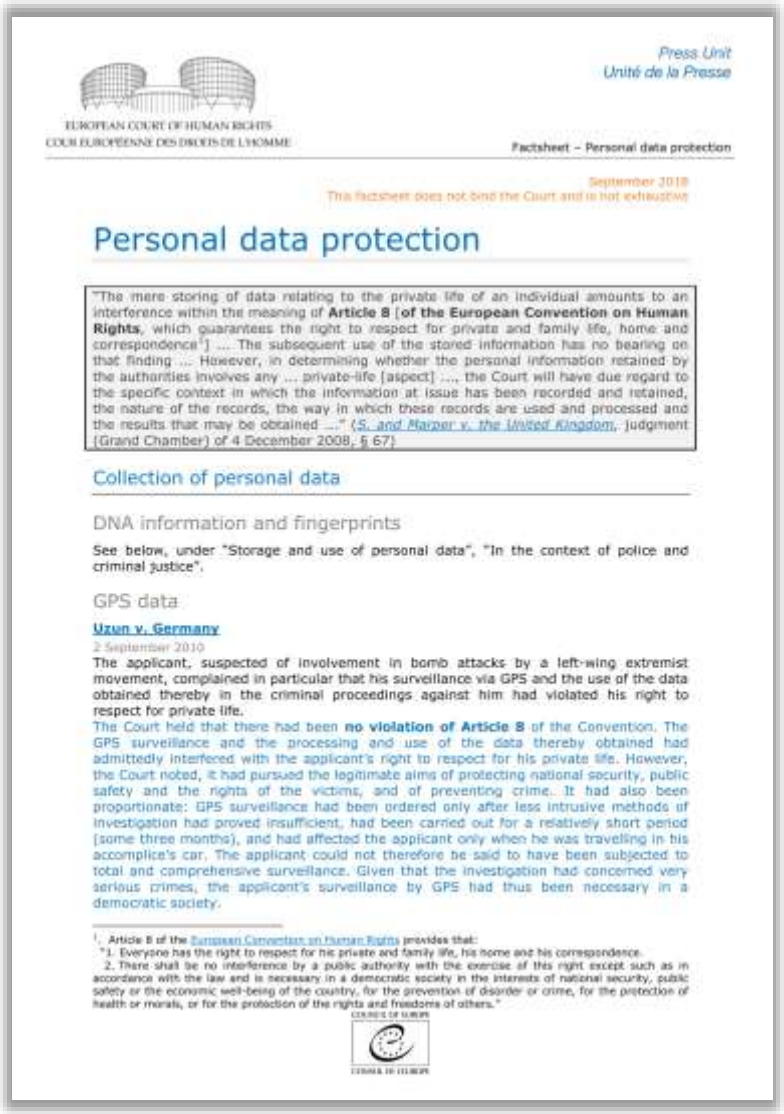
https://www.diepresse.com/5686610/bdquodatenschutz-systematisch-verletztldquo

Судебная практика – базы решений и интересные ситуации



К оглавлению

Обзор судебной практики ECHR по защите персональных данных за 1978-2018 гг.



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

"The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of **Article 8** [**of the European Convention on Human Rights**, which guarantees the right to respect for private and family life, home and correspondence[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 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

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

https://www.coe.int/en/web/data-protection/echr-case-law

259 CJEU об определении совместных контролеров данных



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 page[2] 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

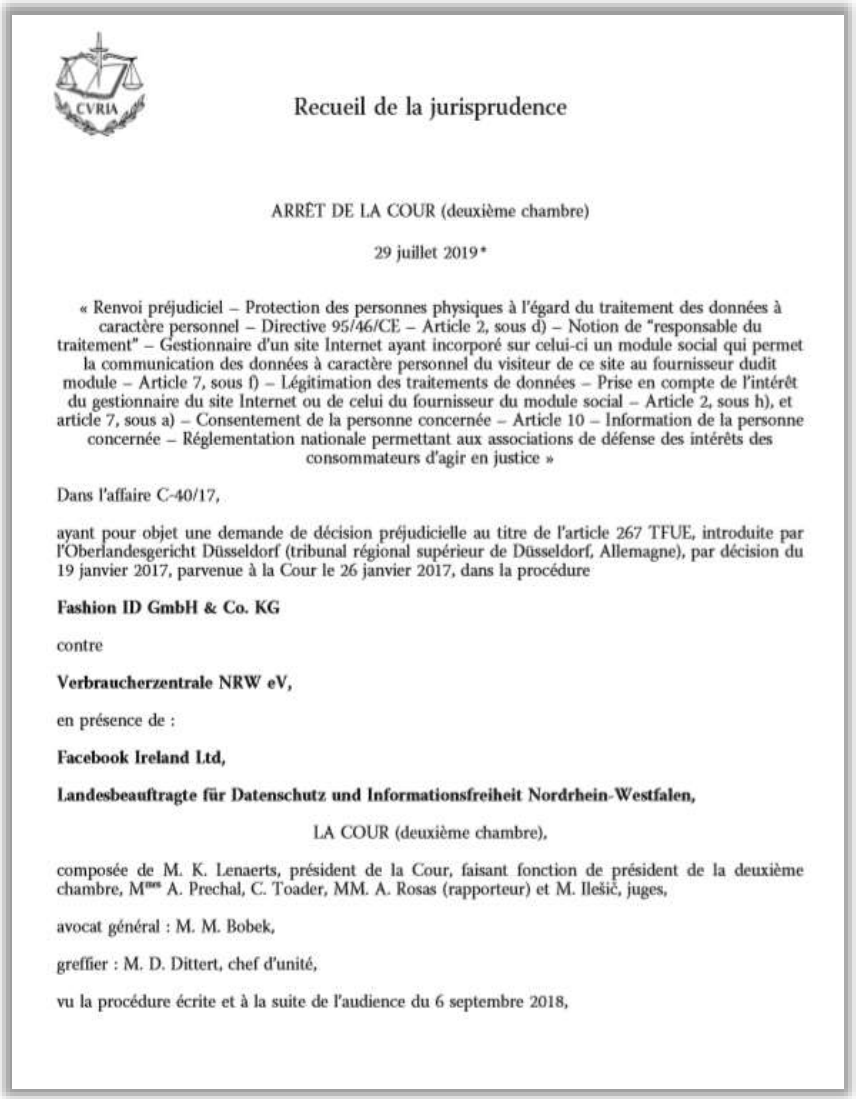
Администратор группы в Facebook совместно с самой социальной сетью является контролером обрабатываемых данных посетителей страницы и несет ответственность за их обработку.

Judgment in Case C-25/17
decision on 10 July 2018
Tietosuojavaltuutettu

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 организовывает, 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=

CJEU о необходимости получать согласия посетителей сайта при размещении на нем социального плагина



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, Mmes A. Prechal, C. Toader, MM. A. Rosas (rapporteur) et M. Ilešič, 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,

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.

Владелец сайта Fashion ID и Facebook признаны совместными контролерами в отношении обработки (сбор и разглашение посредством передачи) данных посетителей указанного сайта при размещении на сайте социального плагина FB в виде веб-кнопки «Нравится». На владельца сайта возложена обязанность информирования посетителей сайта о такой обработке их персональных данных и получения согласия посетителей на нее (включая передачу данных в Facebook). Владелец сайта не несет ответственность за дальнейшую обработку полученных Facebook персональных данных посетителей.

Нужно учитывать, что решение было принято на основании положений уже не действующей Directive 95/46/EC, но ценна сама позиция суда и описание ситуации.

http://curia.europa.eu/juris/celex.jsf?celex=62017CC0040&lang1=en&type=TXT&ancre=

CJEU о хранении cookies и о предварительно отмеченных флажках для выражения согласия на веб-сайтах



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

Press and Information

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

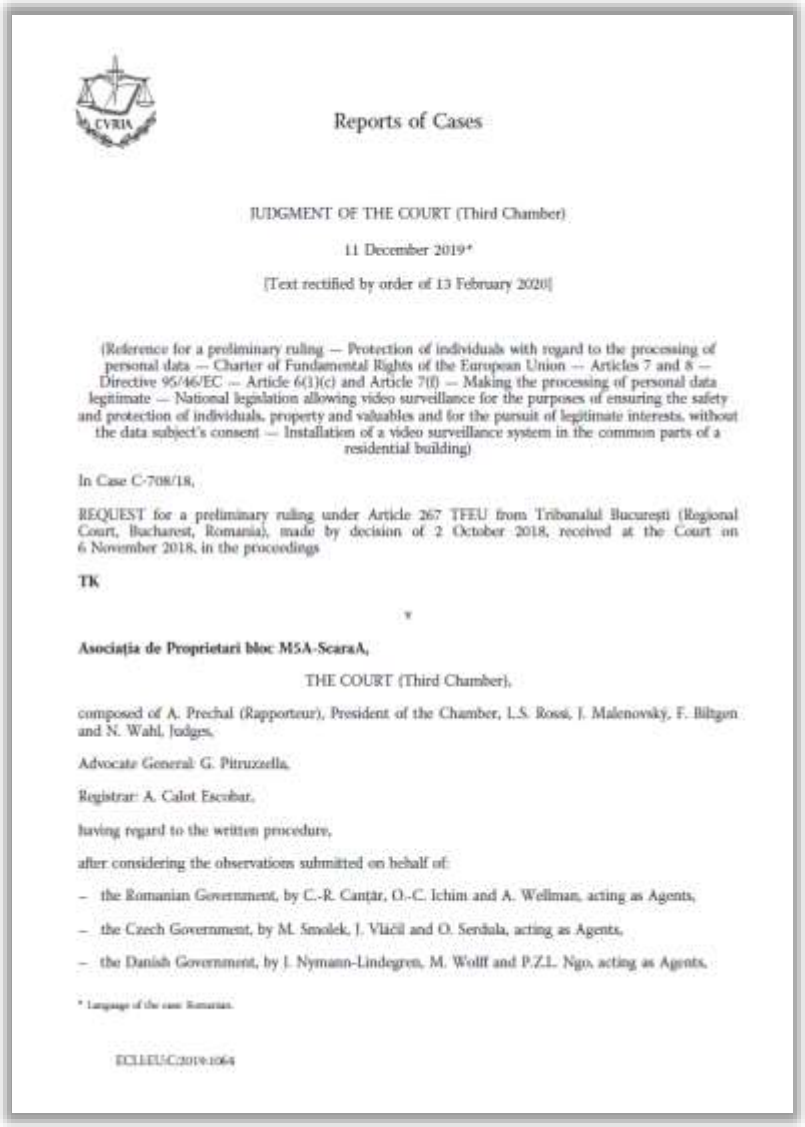
Judgment in Case C-673/17
Bundesverband der Verbraucherzentralen und Verbraucherverbände–
Verbraucherzentrale Bundesverband eV v Planet49 GmbH

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/

CJEU об использовании CCTV на основании законного интереса контроллера



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. Canțăr, 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 Asociaţia 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.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0708&from=EN

Генеральный адвокат CJEU о стандартных договорных условиях (SCC) по делу Schrems II



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

Press and Information

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
Data Protection Commissioner v
Facebook Ireland Limited,
Maximillian Schrems

Генеральный адвокат CJEU высказал мнение о том, что SCC (standard contractual clauses) не должны быть признаны недействительными, но экспортеры (контролеры) персональных данных из ЕС должны предпринимать необходимые и достаточные меры для обеспечения соблюдения SCC со стороны импортеров данных, находящихся за пределами ЕС. В частности, экспортер данных должен самостоятельно оценить, способен ли импортер данных выполнять все требования SCC.

https://www.bakermckenzie.com/en/insight/publications/2019/12/gdpr-international-data-transfer-solutions

Генеральный адвокат CJEU о хранении копий идентификационных документов



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

Press and Information

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-61/19
Orange România SA v
Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)

Генеральный адвокат CJEU Мацей Шпунар (Maciej Szpunar) 05.03.2020 вынес заключение 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. Шпунар 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).

http://curia.europa.eu/juris/document/document.jsf?text=&docid=224083

Административный суд Марселя признал незаконным использование системы распознавания лиц в школах



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

(9ème chambre)

M. Pierre-Yves Gonneau
Rapporteur public

Audience du 3 février 2020
Lecture du 27 février 2020

26-07-01-02
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 Cobbthaigh, demandent 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, suivant à la bonne information de la population et du conseil régional ;

Tribunal Administratif de Marseille

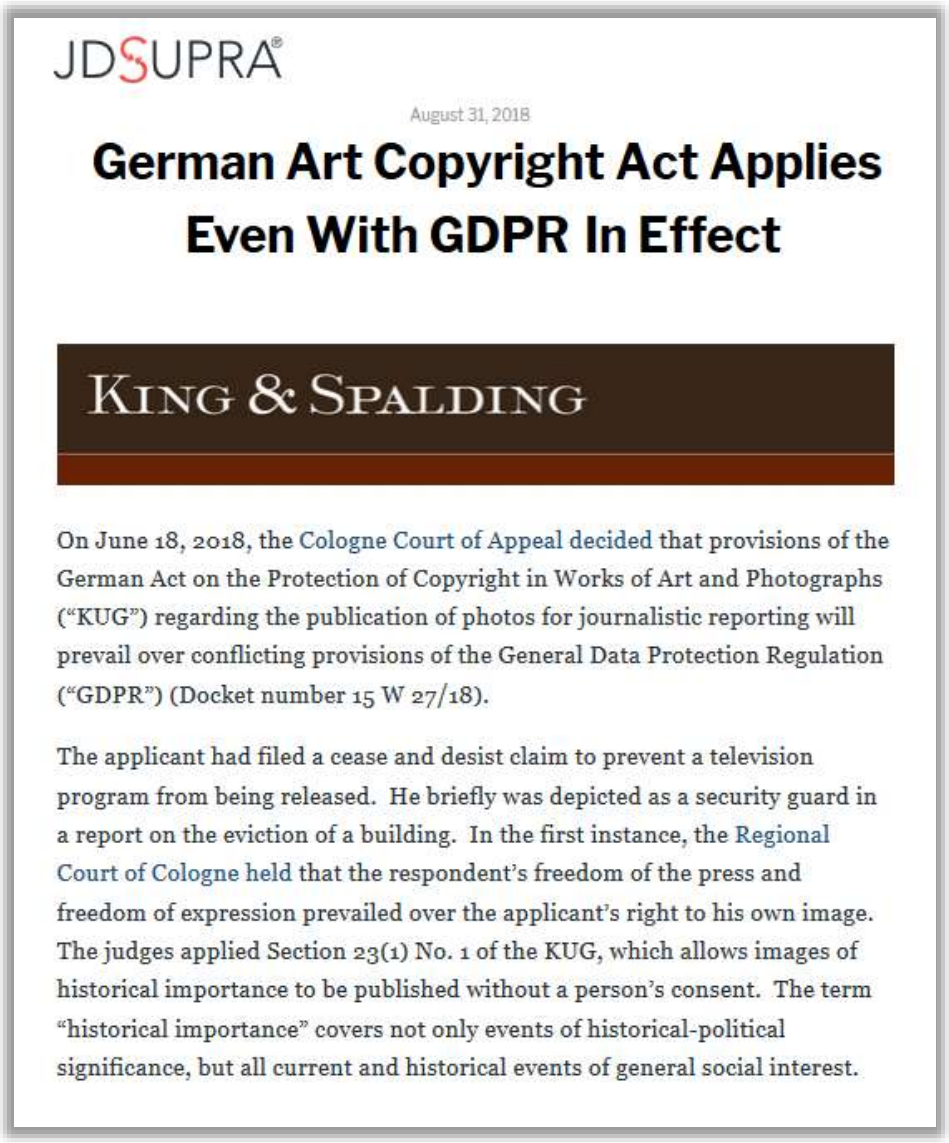
Административный суд Марселя 03.02.2020 признал незаконным использование системы распознавания лиц на входах в школах Ницце и Марселе. Указанные системы были внедрены на основании решения администрации региона «Прованс-Альпы-Лазурный Берег» (Provence-Alpes-Côte d'Azur), принятого 12.2019.

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 контроллера 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.

https://www.laquadrature.net/en/2020/02/27/first-success-against-facial-recognition/

266 Отказ GDPR в приоритете: Германия



JDSUPRA

August 31, 2018

German Art Copyright Act Applies Even With GDPR In Effect

KING & SPALDING

On June 18, 2018, the Cologne Court of Appeal decided that provisions of the German Act on the Protection of Copyright in Works of Art and Photographs ("KUG") regarding the publication of photos for journalistic reporting will prevail over conflicting provisions of the General Data Protection Regulation ("GDPR") (Docket number 15 W 27/18).

The applicant had filed a cease and desist claim to prevent a television program from being released. He briefly was depicted as a security guard in a report on the eviction of a building. In the first instance, the Regional Court of Cologne held that the respondent's freedom of the press and freedom of expression prevailed over the applicant's right to his own image. The judges applied Section 23(1) No. 1 of the KUG, which allows images of historical importance to be published without a person's consent. The term "historical importance" covers not only events of historical-political significance, but all current and historical events of general social interest.

Oberlandesgericht Köln

Case 15 W 27/18

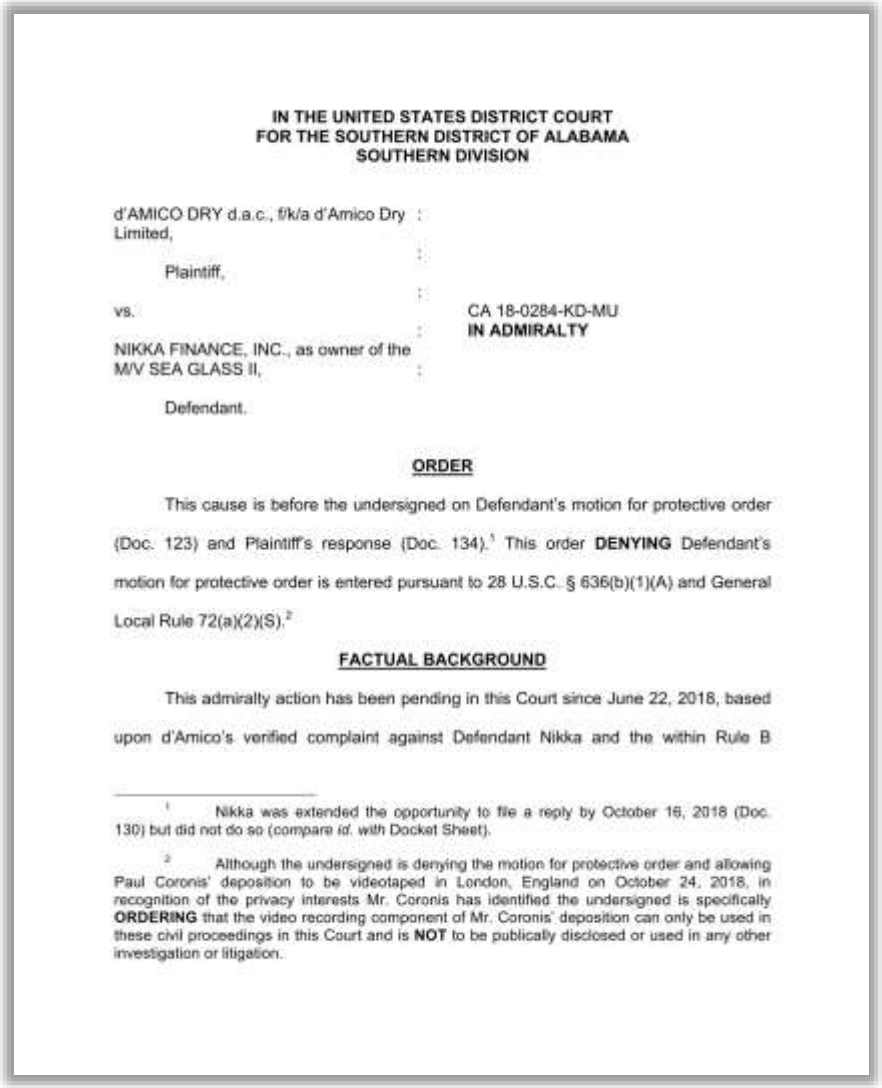
Decision on 18 June 2018

Верховный окружной суд в Кёльне постановил, что положения Закона Германии о защите авторских прав на произведения искусства и фотографии («KUG»), касающиеся публикации фотографий для журналистских репортажей, будут иметь преимущественную силу в отношении положений GDPR.

Суд отказал в удовлетворении иска лица, которое попало на видеозапись репортажа. В первой инстанции суд Кельна постановил, что свобода прессы и свобода выражения мнения ответчика имеют преимущество над правом истца на использование собственного видеоизображения. Судом был применен Раздел 23(1) №1 KUG, который позволяет публиковать изображения исторического значения без согласия запечатлённого на них лица, так как термин «историческое значение» охватывает не только события историко-политического значения, но и все текущие и исторические события, представляющие общественный интерес.

https://www.jdsupra.com/legalnews/german-art-copyright-act-applies-even-68926/

267 Отказ GDPR в приоритете: США



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.

NIKKA FINANCE, INC., as owner of the M/V SEA GLASS II,

Defendant.

CA 18-0284-KD-MU
IN ADMIRALTY

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.

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.

https://law.justia.com/cases/federal/district-courts/alabama/alsdce/1:2018cv00284/62887/140/

268 Google vs «право на забвение»



BBC Sign in | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Google wins landmark right to be forgotten case

By Leo Kelion
Technology desk editor

24 September 2019

The EU's top court has ruled that Google does not have to apply the right to be forgotten globally.

It means the firm only needs to remove links from its search results in Europe - and not elsewhere - after receiving an appropriate request.

The ruling stems from a dispute between Google and a French privacy regulator.

In 2015, CNIL ordered the firm to globally remove search result listings to pages containing damaging or false information about a person.

The following year, Google introduced a geoblocking feature that prevents European users from being able to see delisted links.

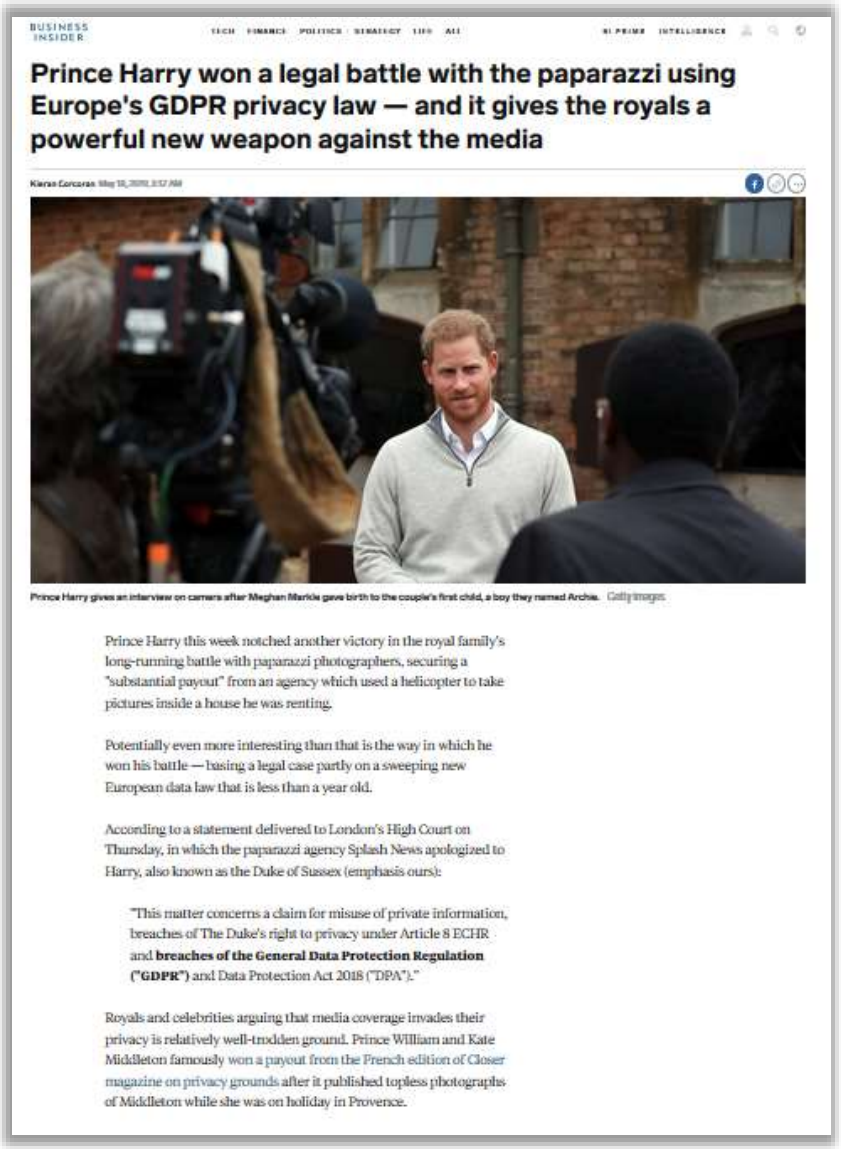
But it resisted censoring search results for people in other parts of the world. And the firm challenged a 100,000 ($109,901; £88,376) euro fine that CNIL had tried to impose.

Court of Justice of the European Union

Европейский суд справедливости (CJEU) поддержал позицию Google в давнем споре с французским регулятором CNIL о локализации права на забвение резидентов ЕС и неправомерности фактического введения режима «глобальной цензуры» путем расширительной интерпретации территориальной сферы применения GDPR. Кроме того, был отменен ранее наложенный на Google штраф в € 100,000.

https://www.bbc.com/news/technology-49808208

269 Использование GDPR против СМИ



BUSINESS INSIDER

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 Corcoran

Prince Harry gives an interview on camera after Meghan Markle gave birth to the couple's first child, a boy they named Archie. Getty Images

Prince Harry this week notched another victory in the royal family's long-running battle with paparazzi photographers, securing a "substantial payout" from an agency which used a helicopter to take pictures inside a house he was renting.

Potentially even more interesting than that is the way in which he won his battle — basing a legal case partly on a sweeping new European data law that is less than a year old.

According to a statement delivered to London's High Court on Thursday, in which the paparazzi agency Splash News apologized to Harry, also known as the Duke of Sussex (emphasis ours):

> "This matter concerns a claim for misuse of private information, breaches of The Duke's right to privacy under Article 8 ECHR and **breaches of the General Data Protection Regulation ("GDPR")** and Data Protection Act 2018 ("DPA")."

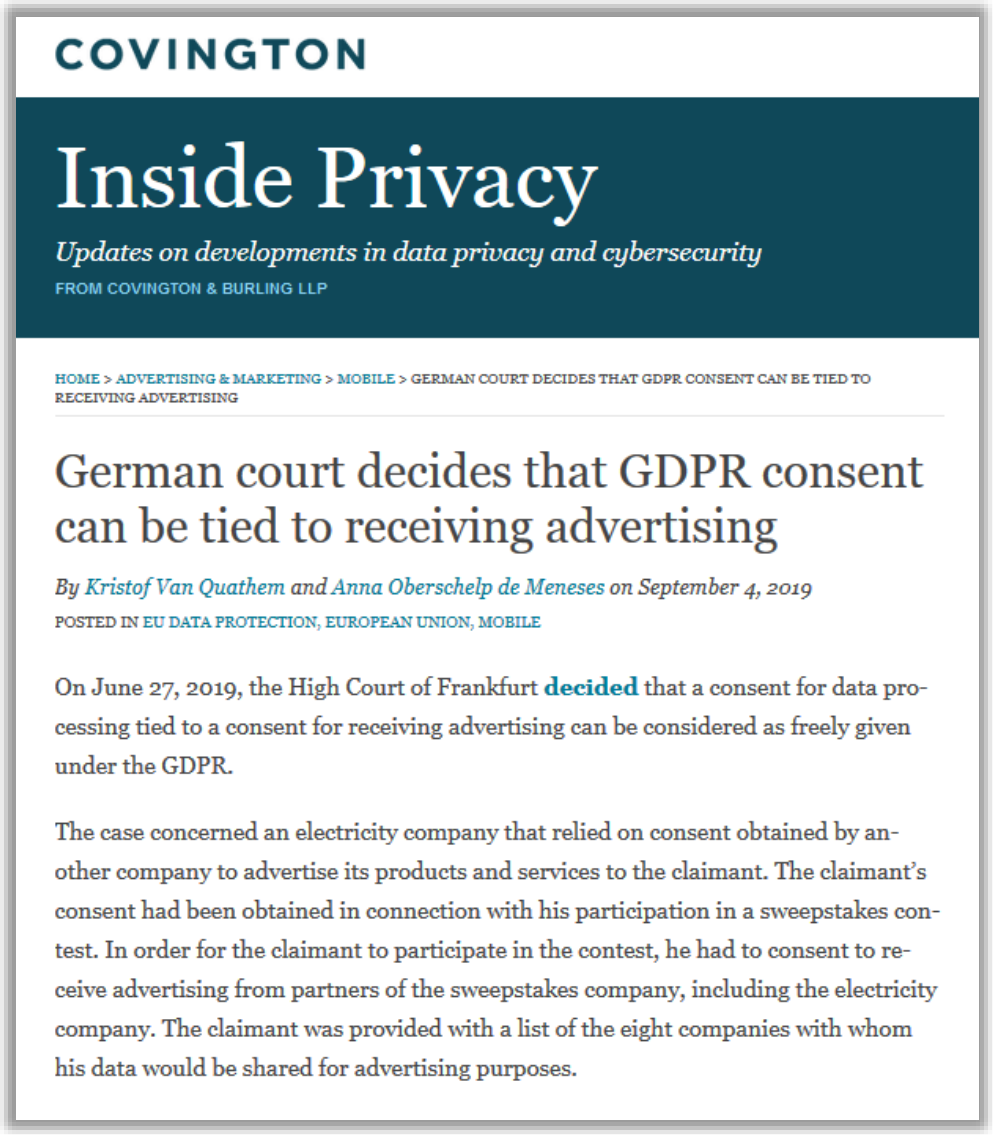
Royals and celebrities arguing that media coverage invades their privacy is relatively well-trodden ground. Prince William and Kate Middleton famously won a payout from the French edition of Closer magazine on privacy grounds after it published topless photographs of Middleton while she was on holiday in Provence.

Принц Гарри одержал победу в судебном споре с фотографами папарацци из агентства Splash News, которое использовало вертолет для фотографирования используемого принцем дома и его окрестностей. В Высоком суде Лондона агентство извинилось перед принцем и согласилось выплатить ему компенсацию за нарушение ст.5 GDPR и британского Закона о защите данных 2018 (DPA) в связи с неправомерной обработкой его персональных данных и нарушением права на неприкосновенность частной жизни.

Согласно мнению Тимоти Пинто, старшего юриста юридической фирмы Taylor Wessing, использование положений GDPR является потенциально привлекательной альтернативой искам о нарушении неприкосновенности частной жизни: «Чтобы преуспеть в иске о диффамации, заявитель должен установить, по крайней мере, что: (i) заявление, на в отношении которого подан иск, дискредитирует истца; и (ii) был нанесен ущерб репутации истца. Напротив, истец, опирающийся на закон о защите данных, не должен доказывать ни одну из этих вещей».

https://www.businessinsider.com/prince-harry-beat-paparazzi-using-gdpr-law-new-royal-weapon-vs-media-2019-5

Плата правом на обработку персональных данных за обещание скидки или участие в лотерее



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

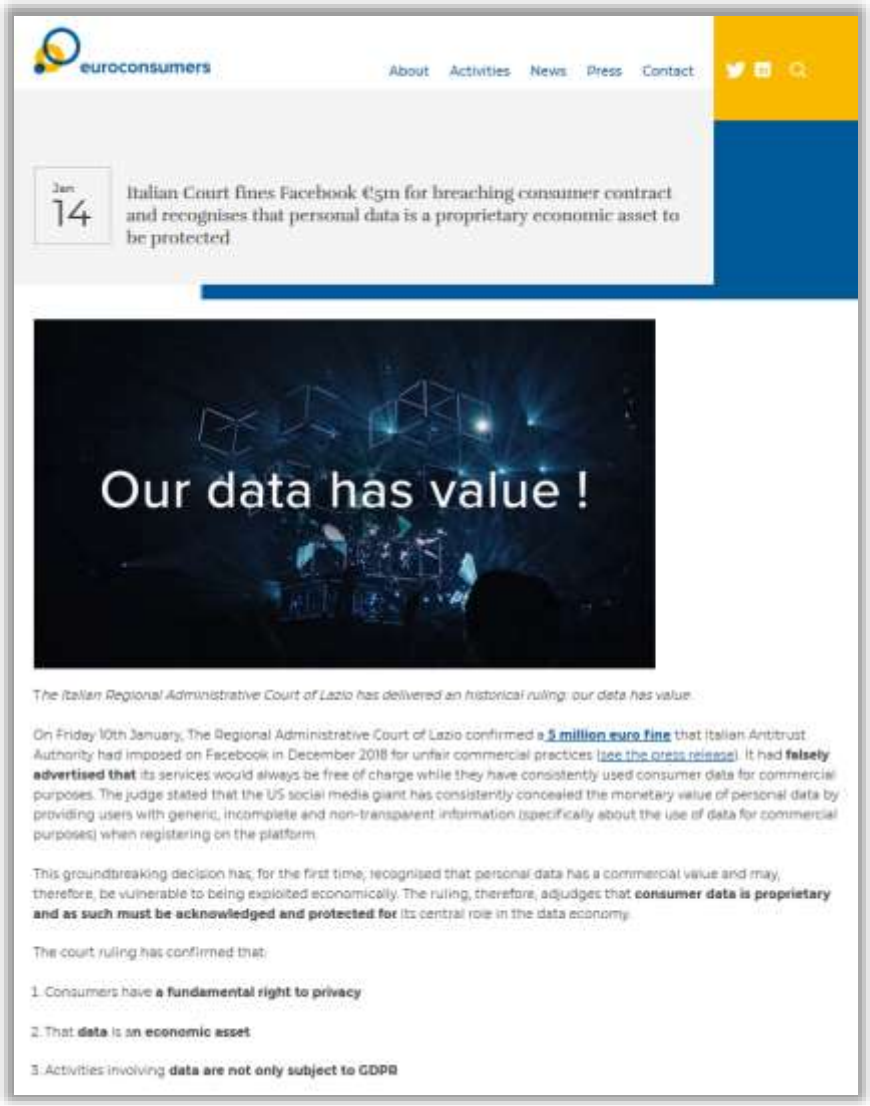
On June 27, 2019, the High Court of Frankfurt **decided** that a consent for data processing tied to a consent for receiving advertising can be considered as freely given under the GDPR.

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».

https://www.insideprivacy.com/advertising-marketing/mobile/german-court-decides-that-gdpr-consent-can-be-tied-to-receiving-advertising

271 Персональные данные имеют экономическое значение



euroconsumers

About Activities News Press Contact

Jan 14

Italian Court fines Facebook €5m for breaching consumer contract and recognises that personal data is a proprietary economic asset to be protected

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.

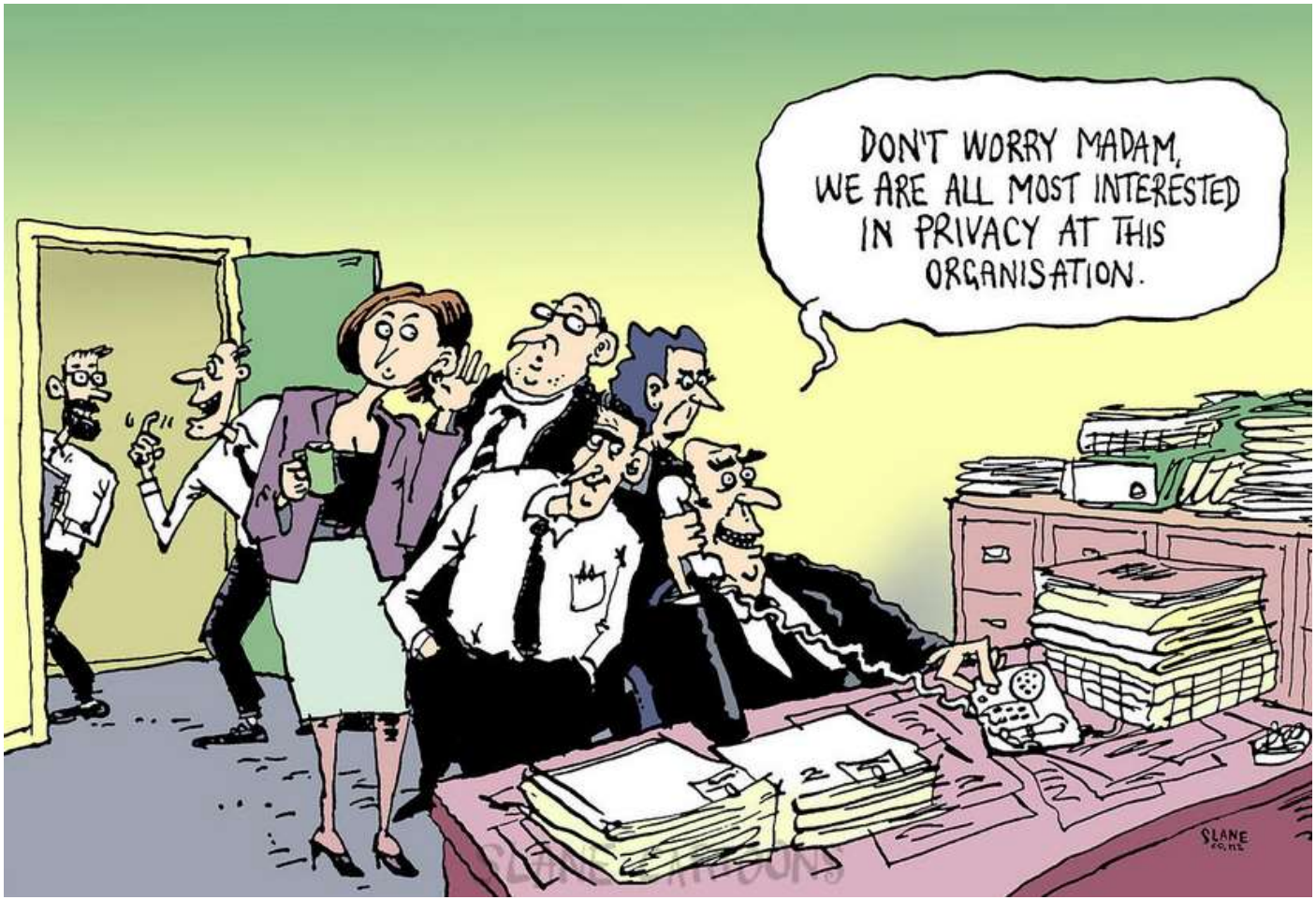
The court ruling has confirmed that:

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.

https://www.euroconsumers.org/news/italian-court-fines-facebook-eur5m-for-breaching-consumer-contract-and

Влияние GDPR на бизнес



К оглавлению

интерфакс INTERFAX ЭКОНОМИКА 08:05, 27 июля 2018

https://www.interfax.ru/business/622756

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 результ 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

bal 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.

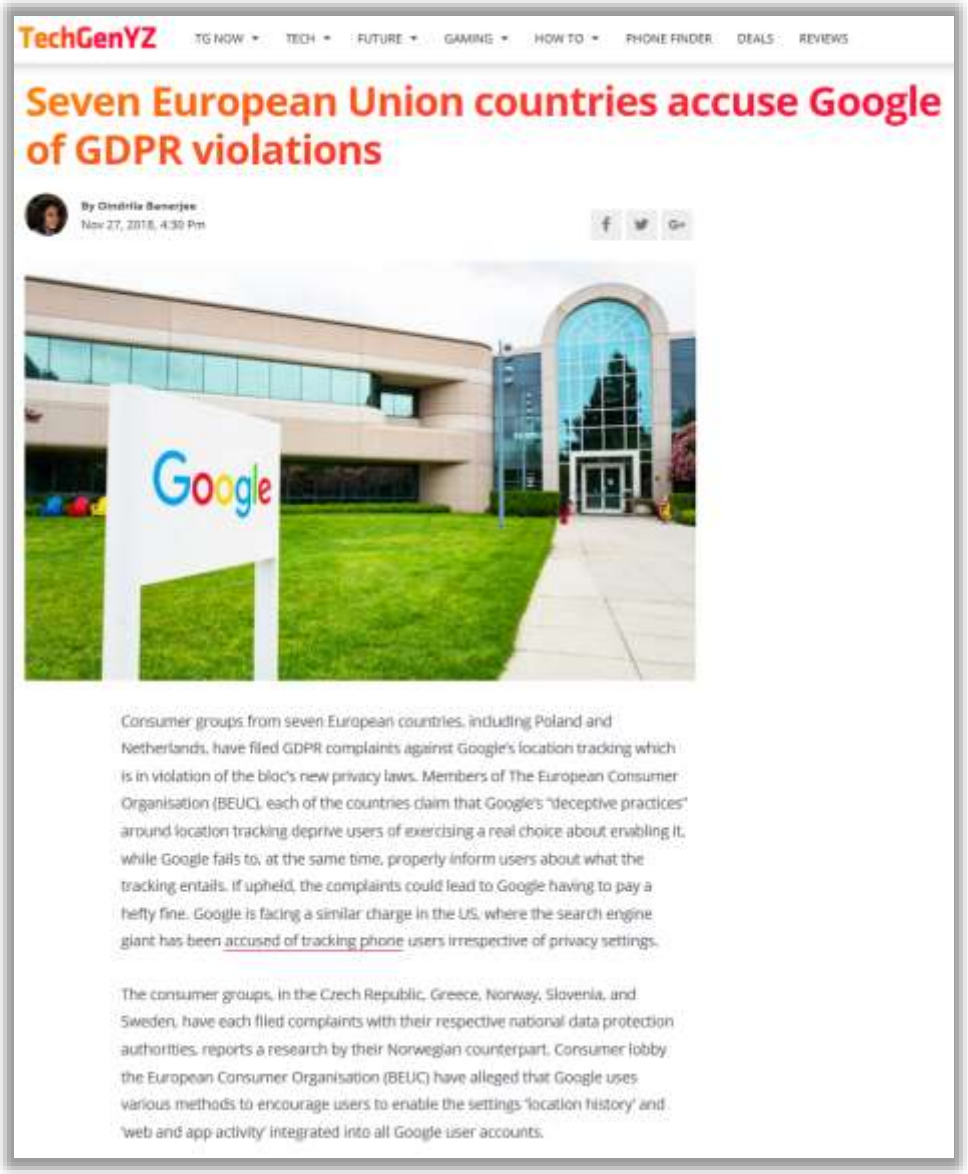
https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law

Исход американского СМБ из европейского рынка по причине неготовности к выполнению требований GDPR

- Brent Ozar, IT consulting services
- CoinTouch, peer-to-peer cryptocurrency exchange
- Drawbridge, cross-device identity service
- FamilyTreeDNA, free and public genetic tools such as Mitosearch and Ysearch
- Gravity Interactive, video game developer (Ragnarok Online, Dragon Saga)
- Hitman: Absolution, video game developed by IO Interactive
- Klout, social reputation service by Lithium
- Loadout, video game developed by Edge of Reality
- Monal, XMPP chat app
- MotoSport, powersports retailer
- Parity, know-your-customer service for initial coin offerings (ICOs)
- Payver, dashcam app
- Pottery Barn, housewares retailer
- Seznam, social network for students
- Steel Root, cybersecurity and IT services
- StreetLend, tool sharing platform for neighbors
- Super Monday Night Combat (SMNC), video game developed by Uber Entertainment
- Tunngle, video game VPN
- Unroll.me, inbox management app
- Verve, mobile programmatic advertising
- Williams-Sonoma, housewares retailer

https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/

275 Проблемы Google



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) обвини 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.

https://www.techgenyz.com/2018/11/27/google-gdpr-violations/

276 Open Data Initiative



REUTERS World Business Markets Politics TV

TECHNOLOGY NEWS SEPTEMBER 24, 2018 / 4:35 PM / 4 DAYS AGO

SAP, Microsoft and Adobe announce data alliance

FRANKFURT (Reuters) - Business software companies SAP, Microsoft and Adobe said on Monday they were forming a data alliance that will make it easier for clients running their applications to get a better overview of the customer.

The partners announced the Open Data Initiative at a Microsoft conference in Orlando, Florida, saying it would help break down information silos that make it hard for businesses to make the most of their customer base.

"The core focus of the Open Data Initiative is to eliminate data silos and enable a single view of the customer, helping companies to better govern their data and support privacy and security initiatives," the three said in a joint statement.

The initiative will enhance interoperability and data exchange between their platforms - Adobe Experience Cloud and Adobe Experience Platform, Microsoft Dynamics 365 and SAP C/4HANA and S/4HANA - through a common model, the partners said.

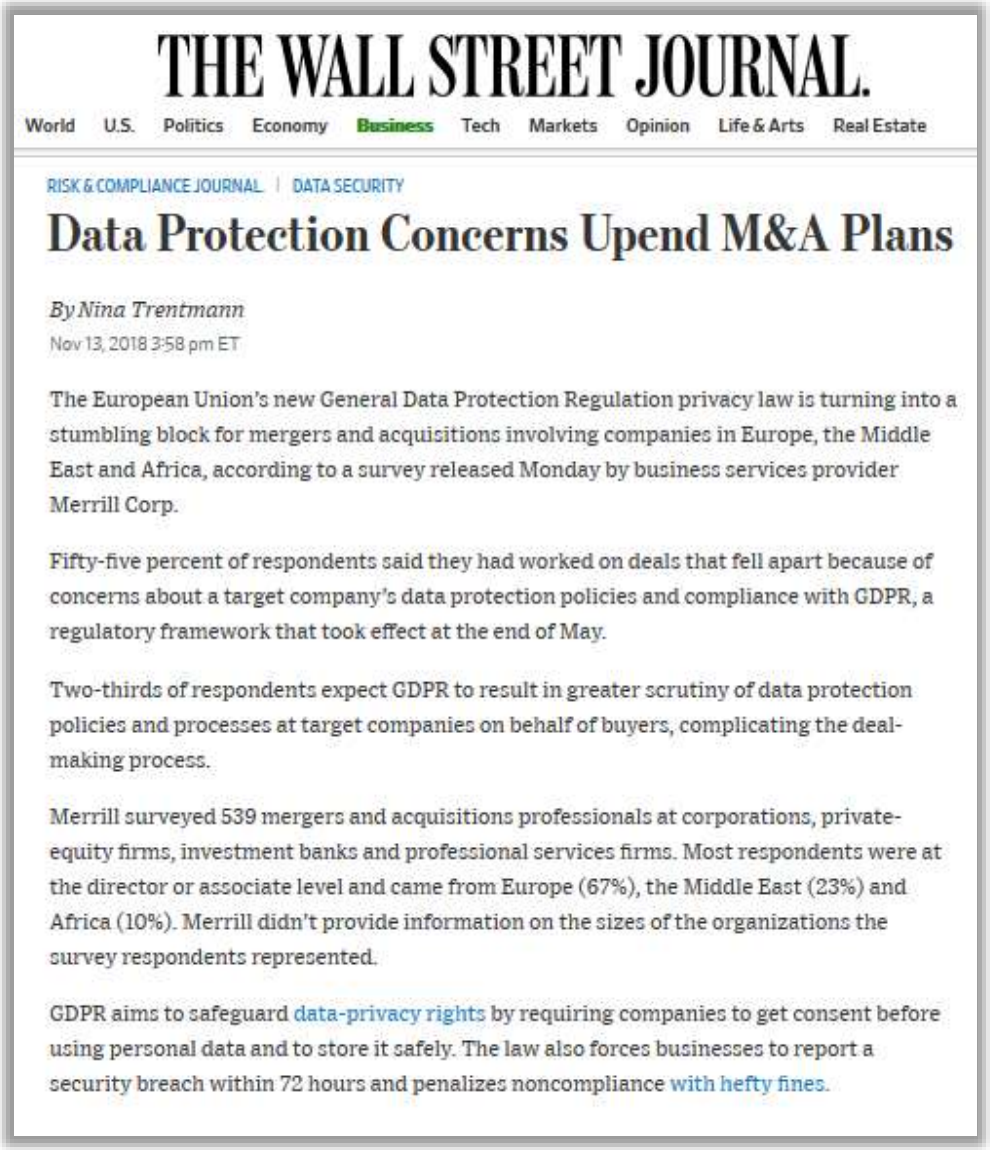
It comes as a new European data privacy law, the General Data Protection Regulation (GDPR), puts a premium on access to customer data given by consent, structurally favoring direct marketing channels over the advertising ecosystem that relies heavily on tracking users online.

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

Негативное влияние GDPR на сделки по слиянию и поглощению



THE WALL STREET JOURNAL.

World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate

RISK & COMPLIANCE JOURNAL | DATA SECURITY

Data Protection Concerns Upend M&A Plans

By Nina Trentmann

Nov 13, 2018 3:58 pm ET

The European Union's new General Data Protection Regulation privacy law is turning into a stumbling block for mergers and acquisitions involving companies in Europe, the Middle East and Africa, according to a survey released Monday by business services provider Merrill Corp.

Fifty-five percent of respondents said they had worked on deals that fell apart because of concerns about a target company's data protection policies and compliance with GDPR, a regulatory framework that took effect at the end of May.

Two-thirds of respondents expect GDPR to result in greater scrutiny of data protection policies and processes at target companies on behalf of buyers, complicating the deal-making process.

Merrill surveyed 539 mergers and acquisitions professionals at corporations, private-equity firms, investment banks and professional services firms. Most respondents were at the director or associate level and came from Europe (67%), the Middle East (23%) and Africa (10%). Merrill didn't provide information on the sizes of the organizations the survey respondents represented.

GDPR aims to safeguard data-privacy rights by requiring companies to get consent before using personal data and to store it safely. The law also forces businesses to report a security breach within 72 hours and penalizes noncompliance with hefty fines.

Согласно опросу, опубликованному в ноябре 2018 г. провайдером бизнес-услуг Merrill Corp., GDPR становится камнем преткновения для слияний и поглощений с участием компаний в Европе, на Ближнем Востоке и в Африке.

Пятьдесят пять процентов респондентов заявили, что работали над сделками, которые развалились из-за опасений относительно состояния защиты данных в целевых компаниях и их соответствиях требованиям GDPR.

Две трети респондентов ожидают, что потенциальные компании-покупатели будут более тщательно подходит к поверке политик и процедур защиты персональных данных в целевых компаниях, что усложнит процесс заключения сделок.

https://blogs.wsj.com/riskandcompliance/2018/11/13/data-protection-concerns-upend-ma-plans/

278 Google – крупнейший бенефициар?



Study: Google is the biggest beneficiary of the GDPR

Thanks to its dominant market position, the industry leader benefits from a stronger concentration in the online advertising market. Although the number of trackers is decreasing overall, a few large tracking operators such as Google receive even more user data.

10.10.2018

Björn Greif
Editor

Blog

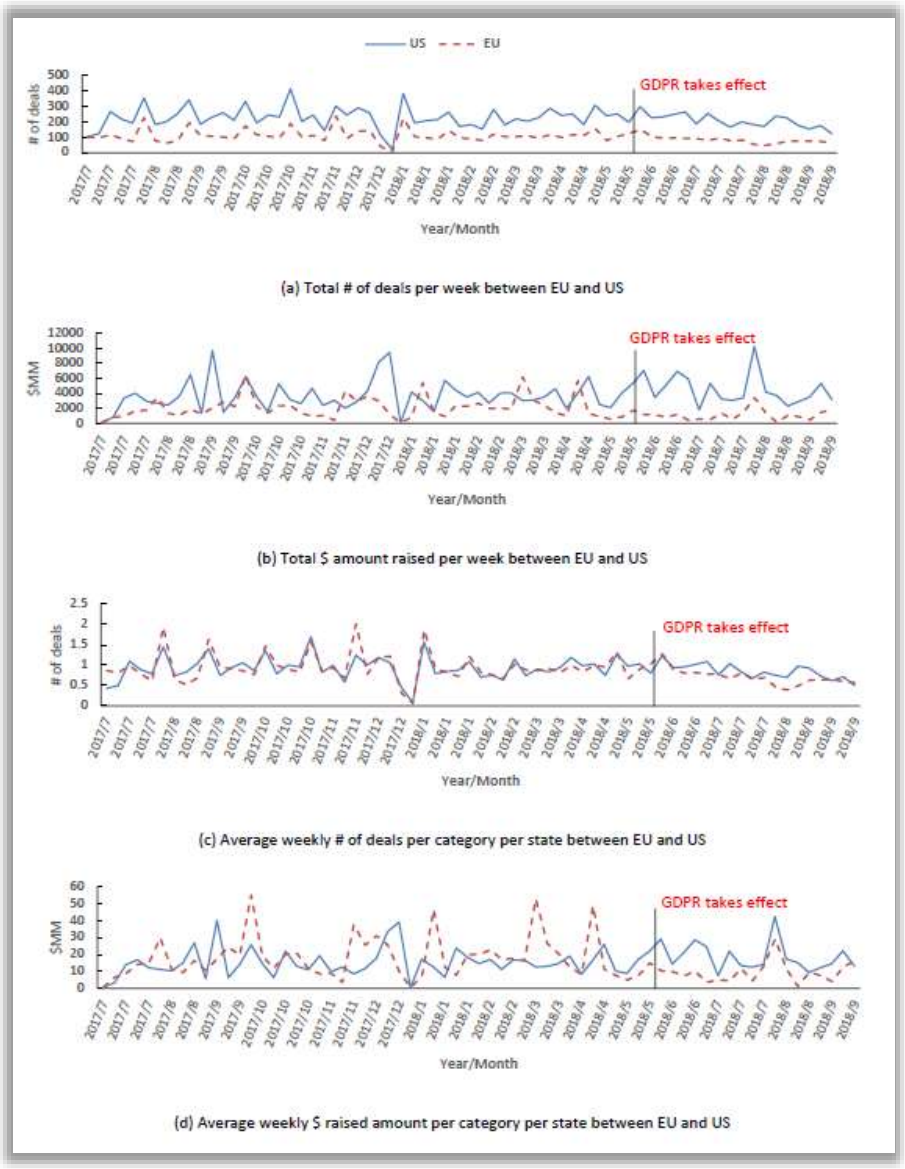
The General Data Protection Regulation (GDPR), which primarily aims to protect personal data within the EU, has been in effect for a little over four months now. But what has changed since 25th of May? What impact did the GDPR have on the tracker landscape and the online advertising market in Europe? 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 операторов компаний-операторов, таких как Google, получают еще больше пользовательских данных.

https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr

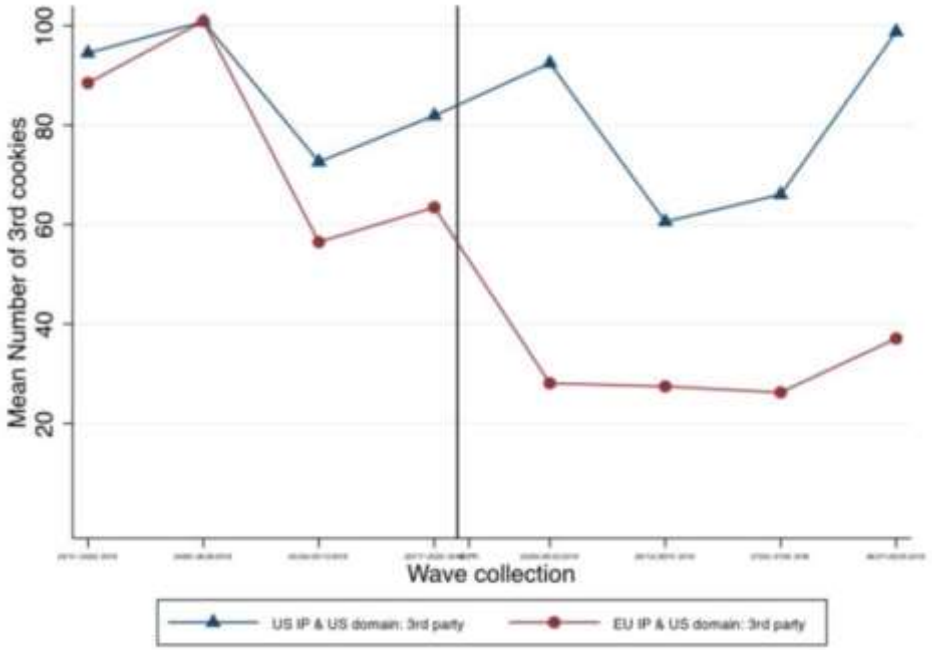
Краткосрочное влияние GDPR на венчурные инвестиции в информационные технологии



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

https://www.nber.org/papers/w25248

Влияние GDPR на контент-провайдеров, существующих за счет рекламы



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.



https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_cheyre_impact_gdpr_on_ad-supported_content_providers.pdf

281 Шантаж компаний посредством GDPR

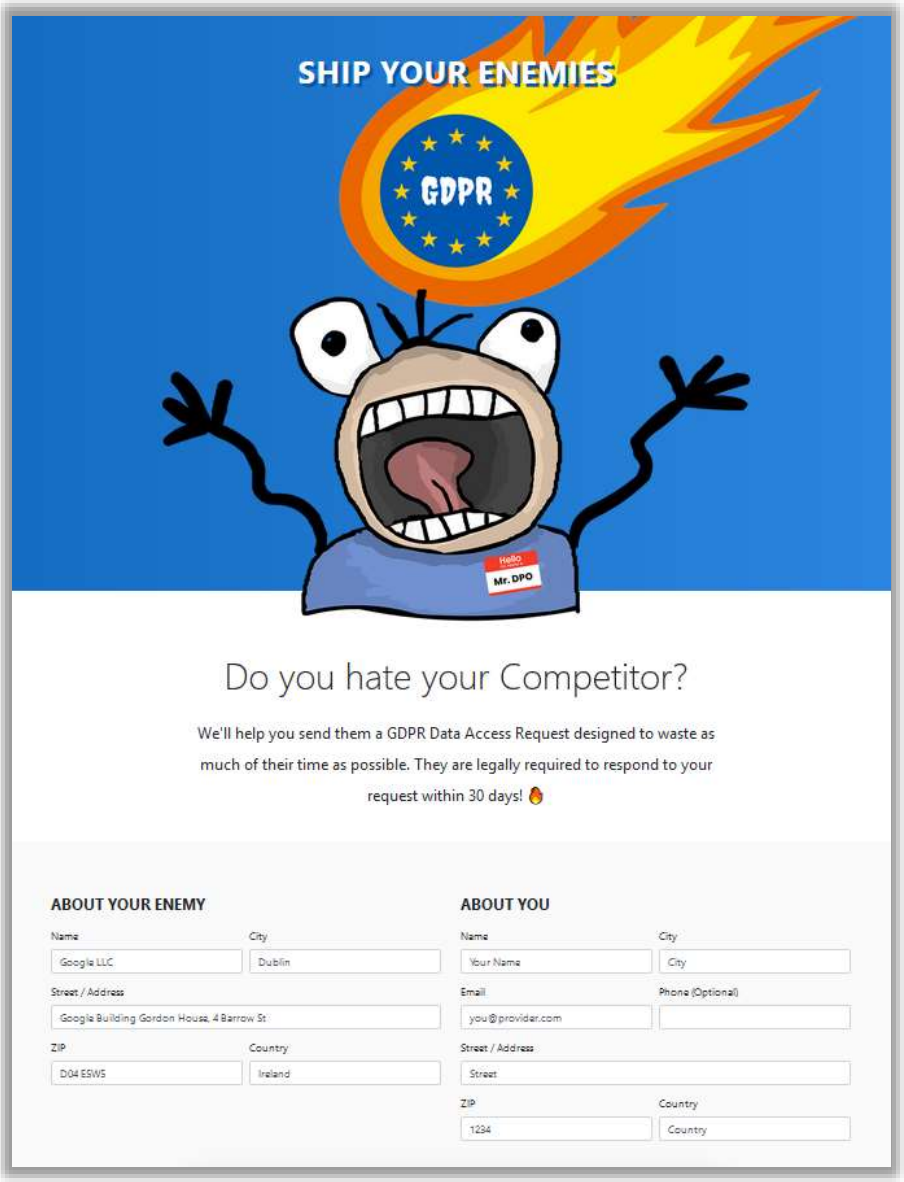


Авторы мошеннической схемы ransomhack используют GDPR для шантажа компаний и получения выкупа

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.

https://www.hackread.com/ransomhack-gdpr-attack-blackmailing-business-owners/

282 Создание административной нагрузки посредством GDPR



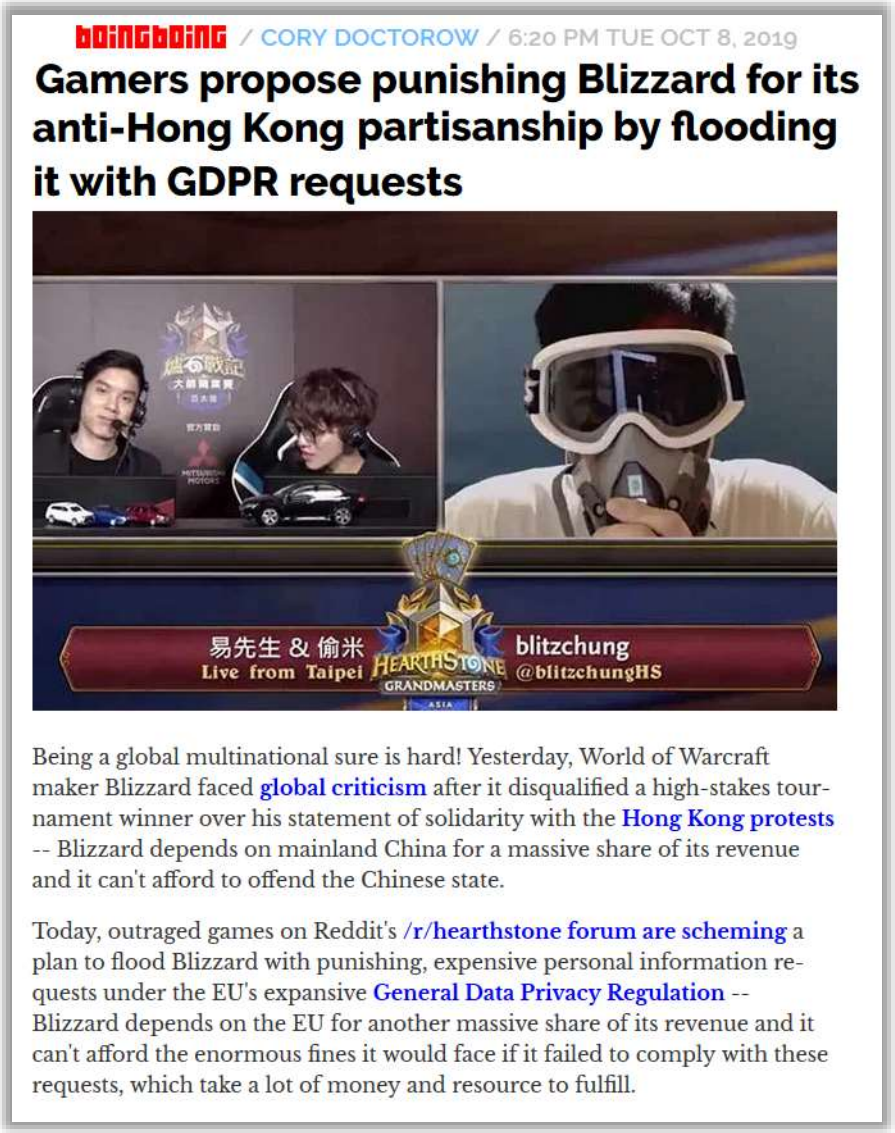
Web-сервис «Ship your enemies»

Автор сайта (Jerre Baum) предлагает всем желающим воспользоваться бесплатным сервисом и направлять от своего имени запросы на доступ к персональным данным, реализую 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.

https://shipyourenemiesgdpr.com/

283 Использование GDPR как орудие общественного давления



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».

https://boingboing.net/2019/10/08/ddos-gdpr.html

Microsoft прислушалось к позиции EDPS в отношении своей роли в качестве контролера



EDPS investigation into IT contracts: stronger cooperation to better protect rights of all individuals

21 Oct 2019

EDPS investigation into IT contracts: stronger cooperation to better protect rights of all individuals

Press Release

Cooperation between public authorities in the Member States, EU institutions and other international organisations is essential to ensure that **contractual arrangements and measures with Microsoft provide the same level of protection for individual rights throughout the European Economic Area (EEA)**. Amended contractual terms, technical safeguards and settings agreed between the Dutch Ministry of Justice and Security and Microsoft to **better protect the rights of individuals** shows that there is significant scope for improvement in the development of contracts between public administration and the most powerful software developers and online service outsourcers. The EDPS is of the opinion that such solutions should be extended not only to all public and private bodies in the EU, which is our short-term expectation, but also to individuals, the Assistant EDPS said today.

In April 2019, the European Data Protection Supervisor (EDPS) launched an investigation into the use of Microsoft products and services by EU institutions. The investigation identified the Microsoft products and services used by the EU institutions and assessed whether the contractual agreements concluded between Microsoft and the EU institutions are fully compliant with data protection rules. The EDPS also considered whether there were appropriate measures in place to mitigate risks to the data protection rights of individuals when EU institutions use Microsoft products and services.

Европейский инспектор по защите данных (EDPS) от 21 октября 2019 года опубликовал отчет, в котором высказаны серьезные опасения по поводу соблюдения компанией Microsoft требований GDPR и роль Microsoft как процессора данных для публичных органов и организаций ЕС. В этом отчете отмечается, что существует значительный потенциал для улучшения разработки контрактов между публичных 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 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).

https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en
https://blogs.microsoft.com/eupolicy/2019/11/18/introducing-privacy-transparency-commercial-cloud-customers/

Пользователи Google в Великобритании могут быть выведены из-под действия GDPR



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.

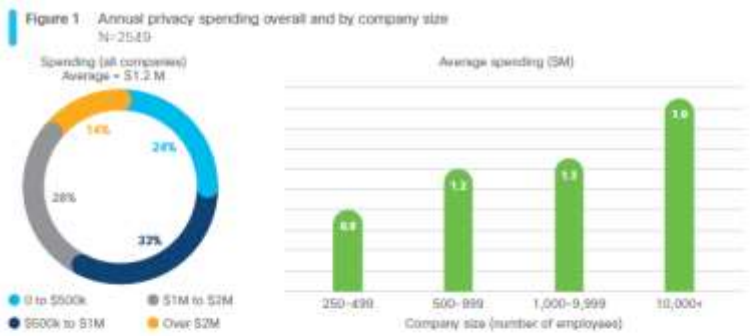
Google has decided to move its British users out of Irish jurisdiction because it is unclear whether Britain will follow GDPR or adopt other rules that could affect the handling of user data, the people said.

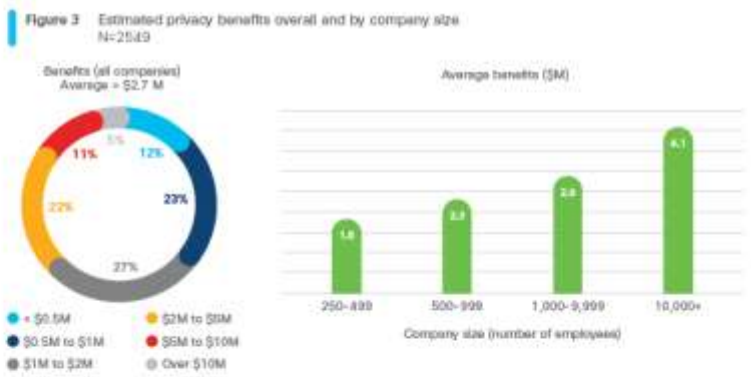
If British Google users have their data kept in Ireland, it would be more difficult for British authorities to recover it in criminal investigations.

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.

https://www.reuters.com/article/us-google-privacy-eu-exclusive-idUSKBN20D2M3

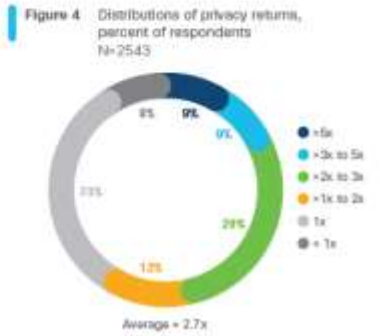
От конфиденциальности к прибыли: достижение положительного дохода от инвестиций в приватность











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.

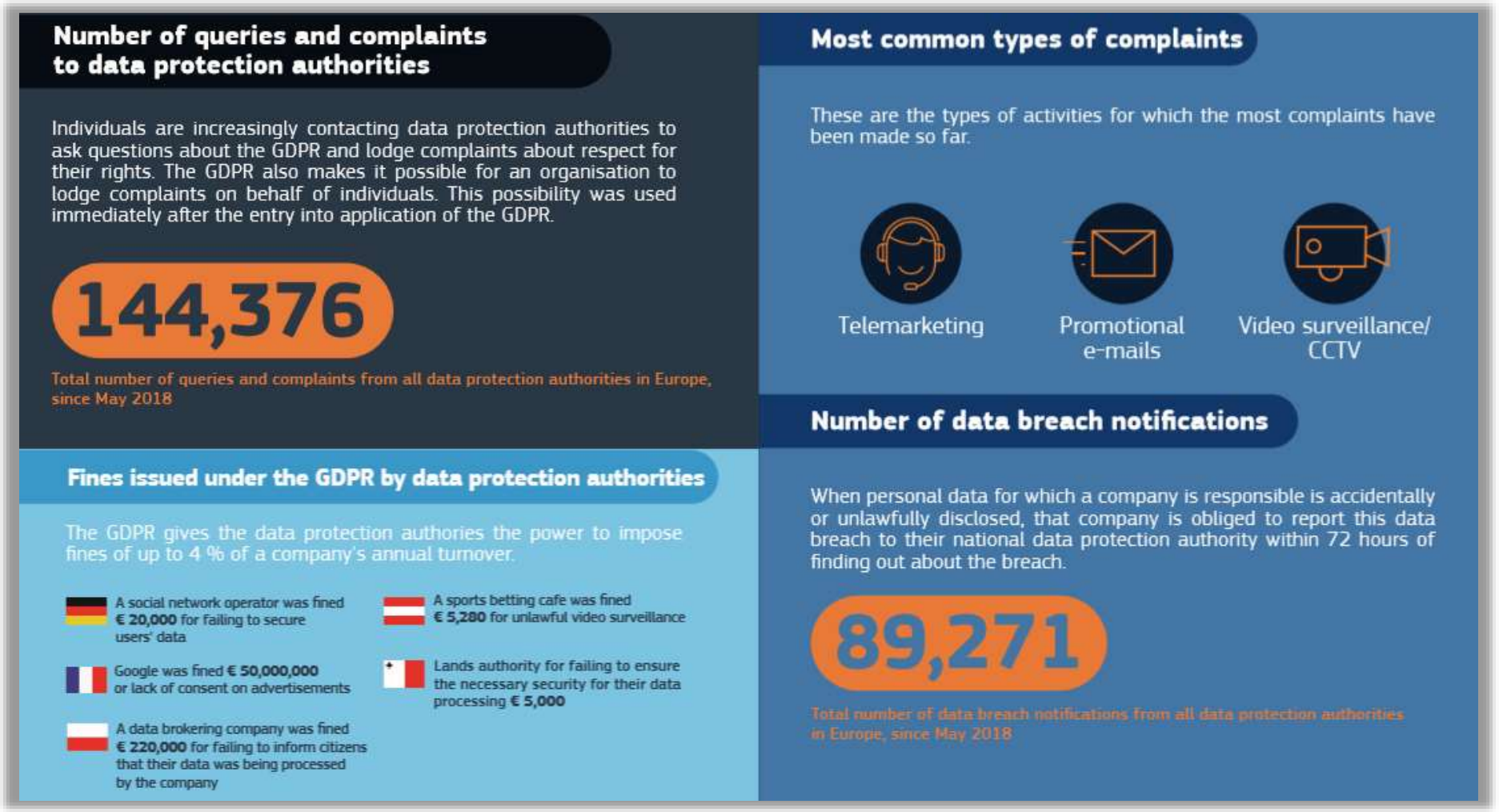
https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf

Итоги применения GDPR в 2018-2019 и дальнейшие перспективы



К оглавлению

288 Итоги первого года GDPR: иконографика от ЕК



https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf

289 €55,955,871 штрафов - итоги 2018 года с GDPR



First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities

Executive Summary

This document sets out an overview of the implementation and enforcement of the General Data Protection Regulation (GDPR) covering both the cooperation mechanism and the consistency findings.

In comparison with the EC Directive 95/46/EC, where Supervisory Authorities (SAs) were working separately even on cross-border cases, the GDPR created a duty for the SAs to cooperate in order to provide a consistent application of the GDPR. In addition to that, the European Data Protection Board (EDPB) provides a consistency mechanism to further foster the harmonisation.

Nine months after the entry into application of the GDPR, the members of the EDPB are of the opinion that the GDPR cooperation and consistency mechanism work quite well in practice. The national supervisory authorities make daily efforts to facilitate this cooperation, which implies numerous exchanges (written and oral) between them.

These cooperation duties lead to extra workloads, additional time dealing with cases and have an impact on the budget of the regulators. The handling of cross border cases takes time, due to the cooperation, to the need to carry out thorough investigations and in order to national procedural rules. The national SAs have to tackle these challenges regarding the harmonized protection and enforcement of the GDPR.

Until now, there are 6 final One-Stop-Shop cases.

The experiences of the EDPB regarding consistency is – up to now – limited, as no dispute resolution through this new EU body was necessary during the reported period.

First overview
on the implementation of the GDPR

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. Почти половина из них (94 622) — по жалобам частных лиц. Ещё 64 864 дела открыли по уведомлению об утечке данных от компаний-виновников происшествия.

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

http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

Права, предоставленные субъектам, не всегда используются во благо

Ст.15 GDPR: Право на доступ

- Amazon отправил 1700 голосовых записей Alexa не тому пользователю после запроса данных. (The Verge)
- Злоумышленник взломал аккаунт Spotify и получил все сведения о владельце аккаунта, просто запросив их. (Jean Yang)

Ст.17 GDPR: Право быть забытым

- Google пришлось исключить из поисковой выдачи сведения о голландском докторе, который был уволен из-за плохого ухода за пациентом. (NYT)
- Французский мошенник Майкл Франсуа Буджалдон попытается удалить из Интернета любые сведения о судебном разбирательстве против себя, ранее рассмотренным в окружном суде США. (PlainSite)
- СМИ США регулярно получают запросы на удаление статей о судебных процессах в США, касающихся мошенничества, совершенного европейцами. (Mike Masnick)

Ст.20 GDPR: Право на переносимость данных

- Если вы можете перенести свои данные из Facebook в другие приложения, то вы можете сделать то же самое в обратном направлении. И кто же будет иметь преимущество: Facebook или его конкуренты? (Ben Thompson)
- Способы и формы реализации права на переносимость данных, в качестве некоего отраслевого стандарта, могут быть навязаны лидерами отрасли для всех остальных компаний, включая стартапы. (Tyler Cowen)

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

- Запрет компаниям ограничивать предоставление услуг или повышать на них цены для потребителей, которые отказываются от обмена своими персональными данными, поощряет таких потребителей (free riders) и сокращает доступ к бесплатному контенту и услугам для всех остальных. (ITIF)

https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/

Доклад экспертной группы (Multistakeholder Expert group) об итогах применения GDPR в 2018-2019 годах

- Могут ли несовершеннолетние давать согласие или это должны быть их родители - часто неясно. Это может привести к отказу в предоставлении услуг детям и к тому, что дети не смогут выходить в Интернет до тех пор, пока они не достигнут определенного возраста, что не является целью, которую преследует GDPR. (стр. 10)
- Cookie-баннеры, размещаемые на веб-сайтах, часто дают неоднозначную информацию и заставляют пользователей давать согласие на обработку и обмен данными с неопределенными третьими лицами в целях таргетированной рекламы. (стр 10)
- Член (собрания) сообщает об увеличении числа лиц, желающих подать иск в суд для защиты прав субъектов данных. (стр. 11)
- Некоммерческие организации, имеющие право на защиту прав субъектов данных в соответствии со статьей 80 GDPR, начали использовать возможность осуществлять представительские действия по нарушениям GDPR. (стр. 12)
- Некоторые члены считают, что применение GDPR к новым технологиям, таким как блокчейн, большие данные или искусственный интеллект, вызывает вопросы, которые, если их не решить, могут повлиять на развитие таких технологий. (стр. 16)
- Рынок для опытных DPO все еще незрел, и в этой области все еще слишком мало экспертов, принимающих во внимание актуальные потребности организаций. CEDPO (Confederation of the European Data Protection Organisations) обозначает обеспокоенность в связи с появлением множества учебных курсов, которые, как утверждается, позволят неспециалистам стать DPO за очень короткий период времени, что нанесет серьезный ущерб профессии в области защиты данных. По их мнению, есть лица, выступающие в качестве DPO, которые не обладают необходимым опытом. (стр. 17)
- В свете возросшей сложности закона о защите данных, сопровождаемого режимом жестких санкций, наблюдается тенденция к переносу большей части рабочей нагрузки по защите данных в юридический отдел, в то время как DPO остается ответственным за минимальный набор обязательств, указанных в GDPR. (стр. 17)

https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=31527

Отчет Datenschutzkonferenz о правоприменительной практике GDPR в 2018-2019 годах

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 "*Datenschutzschutregelwerke*" (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.

https://www.baden-wuerttemberg.datenschutz.de/evaluierung-ds-gvo-zusammenfassung-der-wesentlichen-ergebnisse/

Подготовка позиции Европейской комиссии по обновлению GDPR

В соответствии со ст.97 GDPR 25 мая 2020 года и каждые четыре года впоследствии Европейская комиссия должна направлять отчет об оценке и пересмотре GDPR в Европейский парламент и Совет ЕС. Сам отчет также должен быть опубликован. В октябре 2019 года был опубликован проект такого отчета, в котором можно выделить следующие аспекты:

- Германия указала на противоречивость и фрагментарность правоприменительной практики GDPR, а Чехия предложила обобщить и опубликовать описание лучших практик;
- Ирландия охарактеризовала подход GDPR к защите детей как фрагментированный и разрозненный, а Франция и Нидерланды требуют установления единого возраста согласия в ЕС;
- Германия и Чехия хотят, чтобы EDPB подготовило единый реестр процессов обработки данных, для которых DPIA (ст.35 GDPR) будет обязательным;
- Германия отметила, что компании хотели бы более быстрой и конкретной помощи со стороны DPA, а субъектам требуется больше советов по Privacy и ускорения обработки своих запросов;
- Германия предложила разработать единые критерии в отношении наложения штрафов;
- Литва предложила уточнить обязательность исполнения судебного решения для DPA, находящегося в другой юрисдикции;
- Болгария и Германия обратили внимание на перегруженность DPA в подготовке ответов на жалобы субъектов в связи с утечками (89,000 на апрель 2019 г.) их данных (ст.33 и ст.77 GDPR);
- Нидерланды представили список стран – потенциальных будущих кандидатов на признание в качестве обеспечивающих адекватный уровень защиты (ст.45(3) GDPR). К ним относятся Сингапур, Колумбия, Мексика, Южная Африка, Сербия и Международный финансовый центр Дубая, а также все страны, которые ратифицировали и внедрили модернизированную Конвенцию 108+;
- Бельгия указала на нежелание применять кодексы поведения (ст.40 GDPR) из-за отсутствия четких руководящих принципов, Болгария назвала кодексы поведения способом получения организациями «индульгенции» 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.

https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf

Законодательные инициативы о персональных данных в ЕС и США



К оглавлению

295 Proposal 2017/0003: GDPR для электронных коммуникаций



EUROPEAN COMMISSION

Brussels, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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)

(Text with EEA relevance)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

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 2017/0228: свободное перемещение обезличенных данных в ЕС



EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 495 final

2017/0228 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a framework for the free flow of non-personal data in the European Union

{SWD(2017) 304 final}
{SWD(2017) 305 final}

Proposal 2017/0228 (COD) for a Regulation on a framework for the free flow of non-personal data in the European Union
Проект Регламента о свободном перемещении неличных данных в ЕС. По расчетам Европейской Комиссии потенциальный эффект от снятия внутренних барьеров ЕС для свободного перемещения информации составит до €739 млрд. к 2020 году, удвоив дою отрасли до 4% ВВП ЕС.

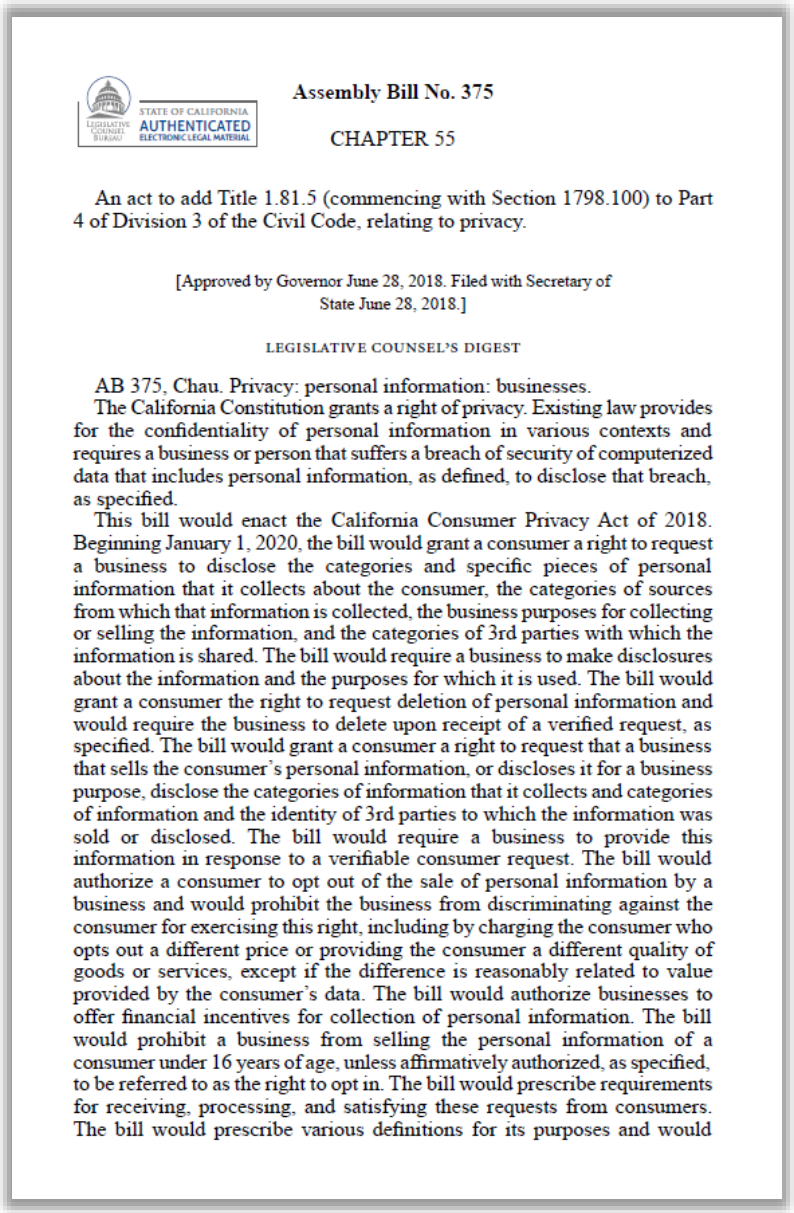
Полезные ссылки:

- Текущий статус рассмотрения проекта
- Общее описание целей, задач, структуры и содержания проекта

Отменяемые требования о локализации данных в ЕС:

- данные о транзакциях при оказании финансовых услуг;
- сведения, составляющие профессиональные тайны (например, врачебная тайна);
- информация, образующаяся в процессе работы государственных органов, вне зависимости от ее критичности.

297 Калифорнийский GDPR



STATE OF CALIFORNIA
AUTHENTICATED
ELECTRONIC LEGAL MATERIAL

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.

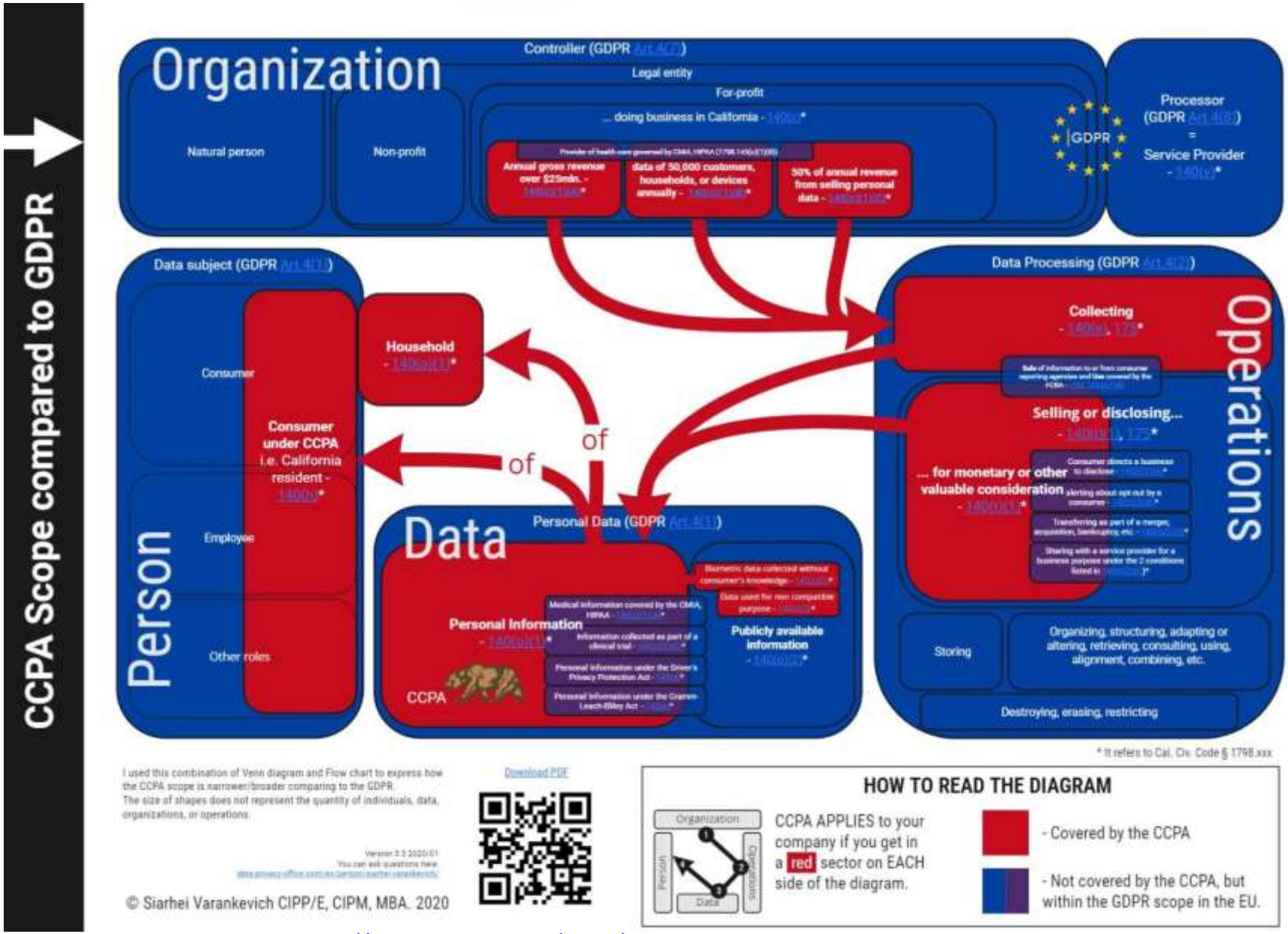
Новый закон вступил в силу **01.01.2020** и **распространяется на крупные компании**, которые соответствуют хотя бы одному из следующих условий:

- 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.

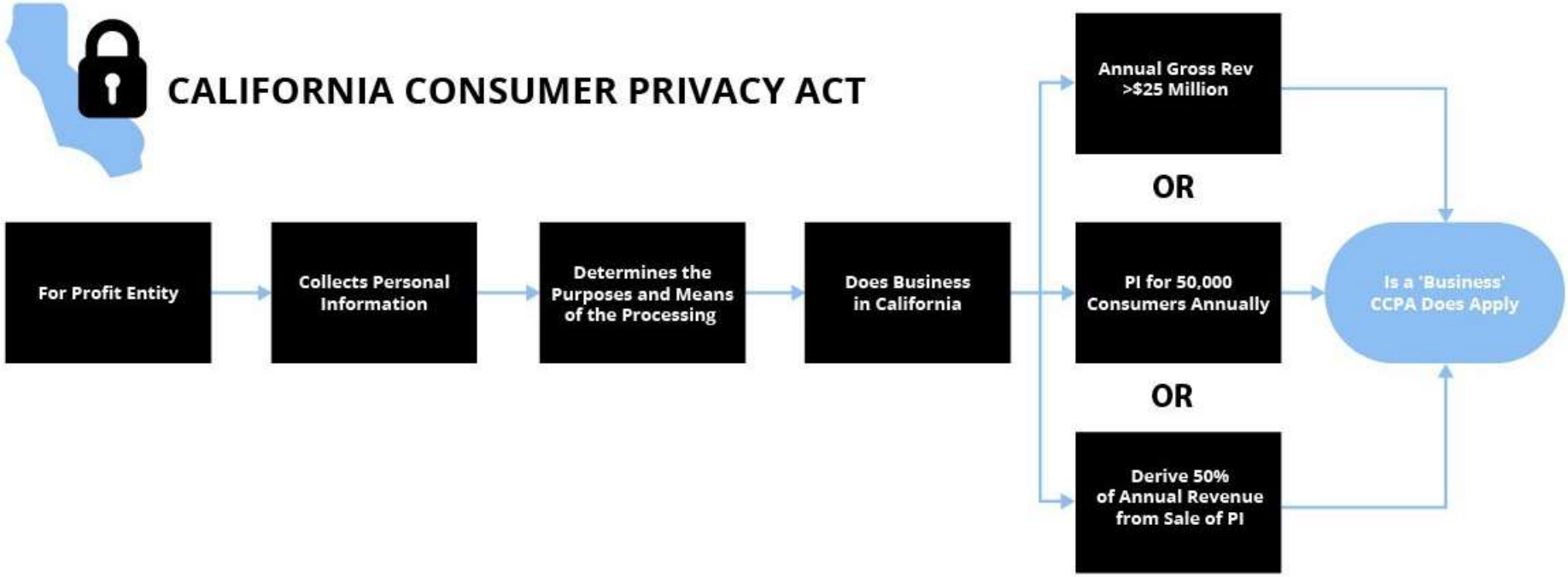
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

298 Область действия CCPA в сравнении с GDPR



https://www.linkedin.com/posts/activity-6637674734647590912-w5Hp

299 Анализ применимости CCPA



https://kofirm.com/ccpa-california-consumer-privacy-act-need-to-know

300 США готовят свой общефедеральный GDPR?

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 общефедерального 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)

https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy

301 США могут пойти своим путем



c|net 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.

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.

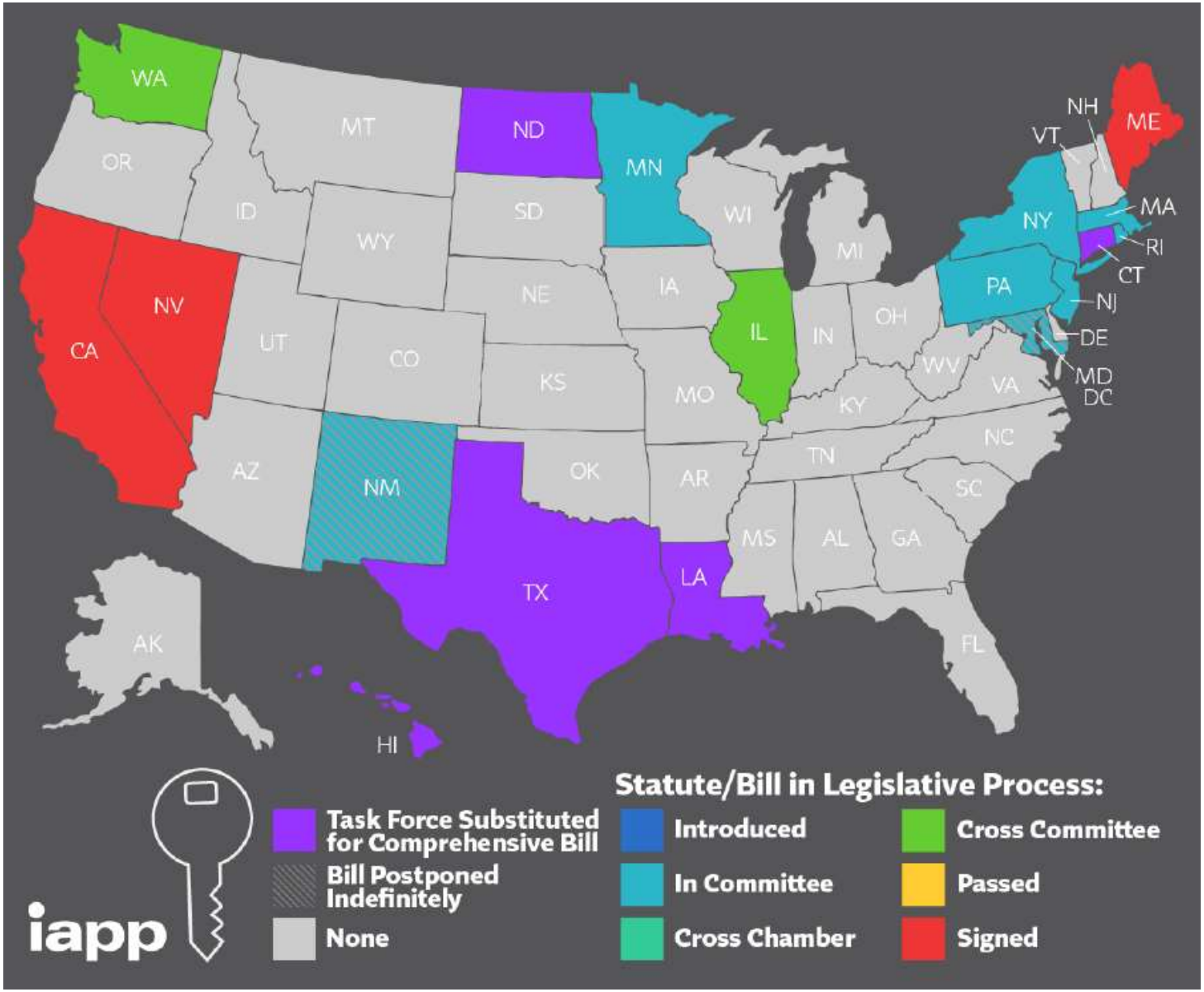
On Tuesday the House Energy and Commerce Committee held its first hearing on data privacy, with a Senate hearing scheduled for Wednesday. Once just a blip on the political radar, data privacy has now set off a roaring alarm, as tech scandals have surfaced regularly over the last few years.

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 CCPA 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.

https://www.cnet.com/news/at-hearing-on-federal-data-privacy-law-debate-flares-over-state-rules/

302 Ситуация по законодательству о Privacy в США на 10.2019



https://iapp.org/resources/article/state-comparison-table/

303 законодательству о Privacy в США на 10.2019

State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	Consumer Rights: To Access to Collected	To Access to Shared	To Rectification	To Deletion	To Restriction	To Portability	To Opt-Out	Against Solely Automated Decision Making	Private Right of Action	Business Obligations: Strict Age-based Opt-In	Notice/Transparency Requirement	Data Breach Notification	Risk Assessment	Prohibition on Discrimination	Purpose Limitation	Processing Limitation	Fiduciary Duty
California		**Ca. Civ. Code §§ 1798.100 - .199**	**California Consumer Privacy Act**	**x**	**x**		**x**		**x**	**x**		**s**	**16**	**x**			**x**			
~~Connecticut~~		~~RB 1108/SB 1108~~																		
Hawaii		*SB 418*[I]		*x*	*x*		*x*		*x*	*x*			*16*	*x*	*x*		*x*			
~~Hawaii~~		~~HCR 225~~																		
Illinois		*HB 3358*	*Data Transparency and Privacy Act*		*x*					*x*				*x*						
~~Louisiana~~		~~HB 249~~																		
Maine		**LD 946** [II]	**An Act To Protect the Privacy of Online Consumer Information**					**x**		**in**				**x**			**x**			
~~Maryland~~		~~SB 613~~	~~Online Consumer Protection Act~~	~~x~~	~~x~~		~~x~~		~~x~~	~~x~~				~~x~~			~~x~~			
Massachusetts		*SD 341/S 120*		*x*	*x*		*x*		*x*	*x*		*x*	*18*	*x*			*x*			
Minnesota		*HF 2917/SF 2912*		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*			*x*		*x*			*x*	
Nevada		**SB 220/Chapter 603A**								**x**				**x**	**x**					
New Jersey		*S2834*			*x*					*x*				*x*			*x*			
~~New Mexico~~		~~SB 176~~	~~Consumer Information Privacy Act~~	~~x~~	~~x~~		~~x~~		~~x~~	~~x~~		~~s~~	~~18~~	~~x~~			~~x~~			
New York		*SB S5642* [III]	*New York Privacy Act*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*		*x*	*x*				*x*	*x*
~~North Dakota~~		~~HB 1485~~																		
Pennsylvania		*HB 1049*	*Consumer Data Privacy Act*	*x*	*x*		*x*			*x*		*s*	*16*	*x*			*x*			
Rhode Island		*HB 5930/S0234*	*Consumer Privacy Protection Act*	*x*	*x*		*x*		*x*	*x*		*x*	*16*	*x*			*x*			
~~Texas~~		~~HB 4390~~ [IV]	~~Texas Privacy Protection Act~~																	
Washington		*SB 5376*	*Washington Privacy Act*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*			*x*	*x*	*x*				

In Session:
MA, NJ, PA

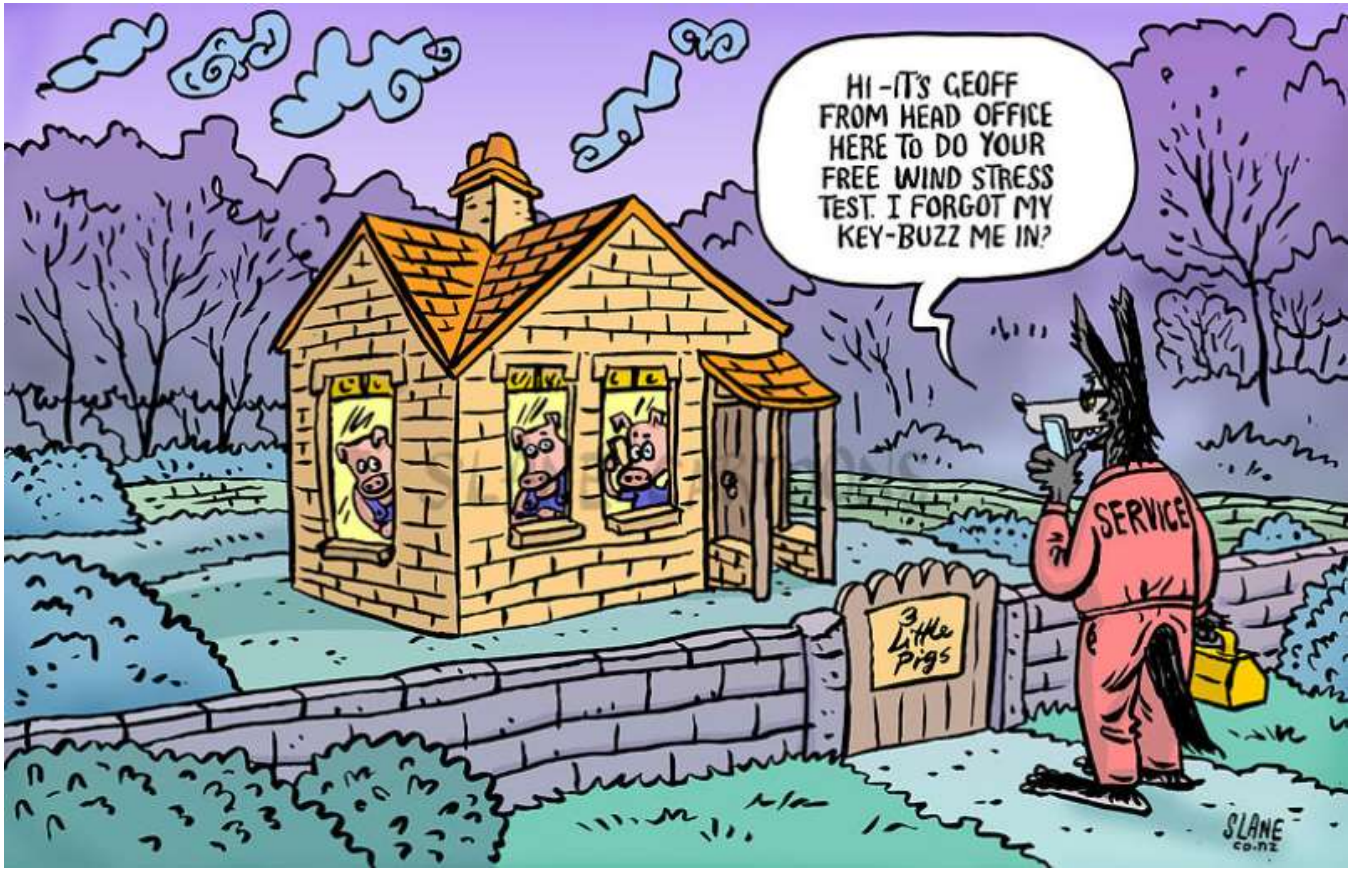
Introduced · In Committee · Crossed Chamber · Cross Committee · Passed · Signed

Bold - passed law
Italics - proposed bill, not passed
s - private right of action for security violations only
in - opt-in consent requirement

~~Black strikethrough - bill postponed indefinitely~~
~~Purple strikethrough - task force substituted for comprehensive bill~~

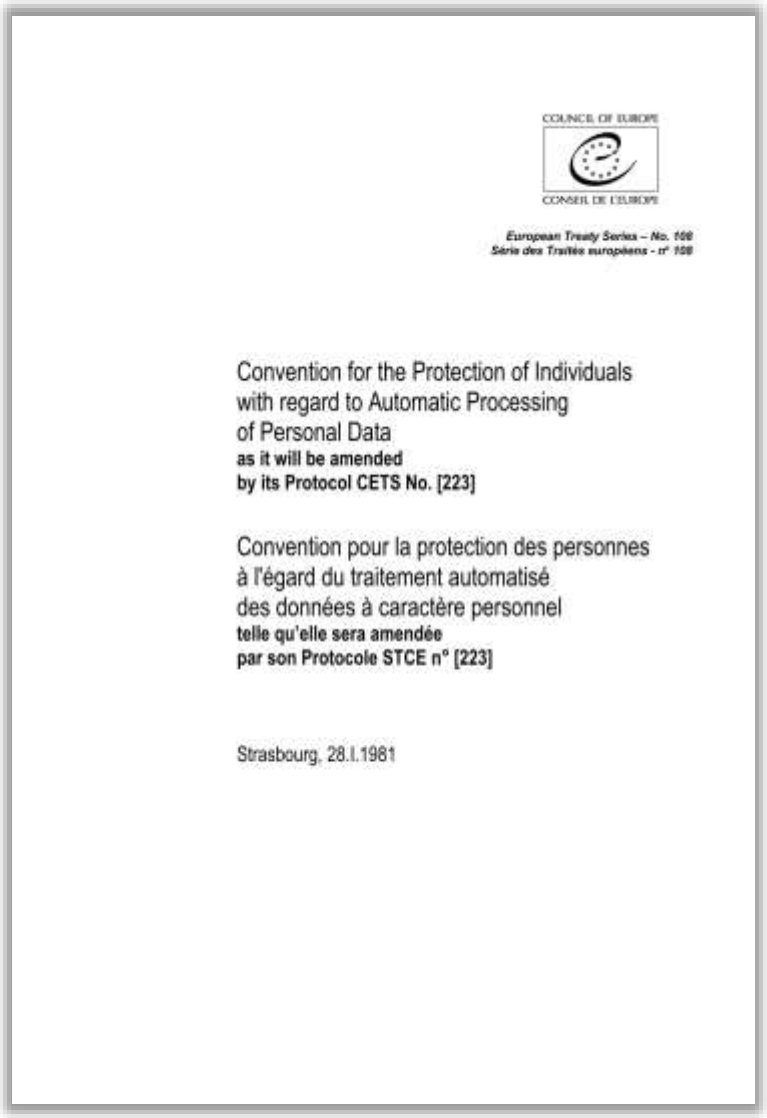
https://iapp.org/resources/article/state-comparison-table/

Модернизация Конвенции 108 и ее влияние на регулирование в РФ



К оглавлению

305 Внесение изменений в Конвенцию 108



COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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

306 Последствия принятия Конвенции 108+ для России



РАСПОРЯЖЕНИЕ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О подписании Протокола о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных

Принять предложение Правительства Российской Федерации о подписании Протокола о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных.

МИДу России подписать от имени Российской Федерации указанный Протокол.

КАНЦЕЛЯРИЯ

Президент Российской Федерации В.Путин

10 октября 2018 года
№ 294-рп

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.

307 Роскомнадзор о последствиях принятия Конвенции 108+



Какие главные изменения могут быть внесены в российскую нормативно-правовую базу?

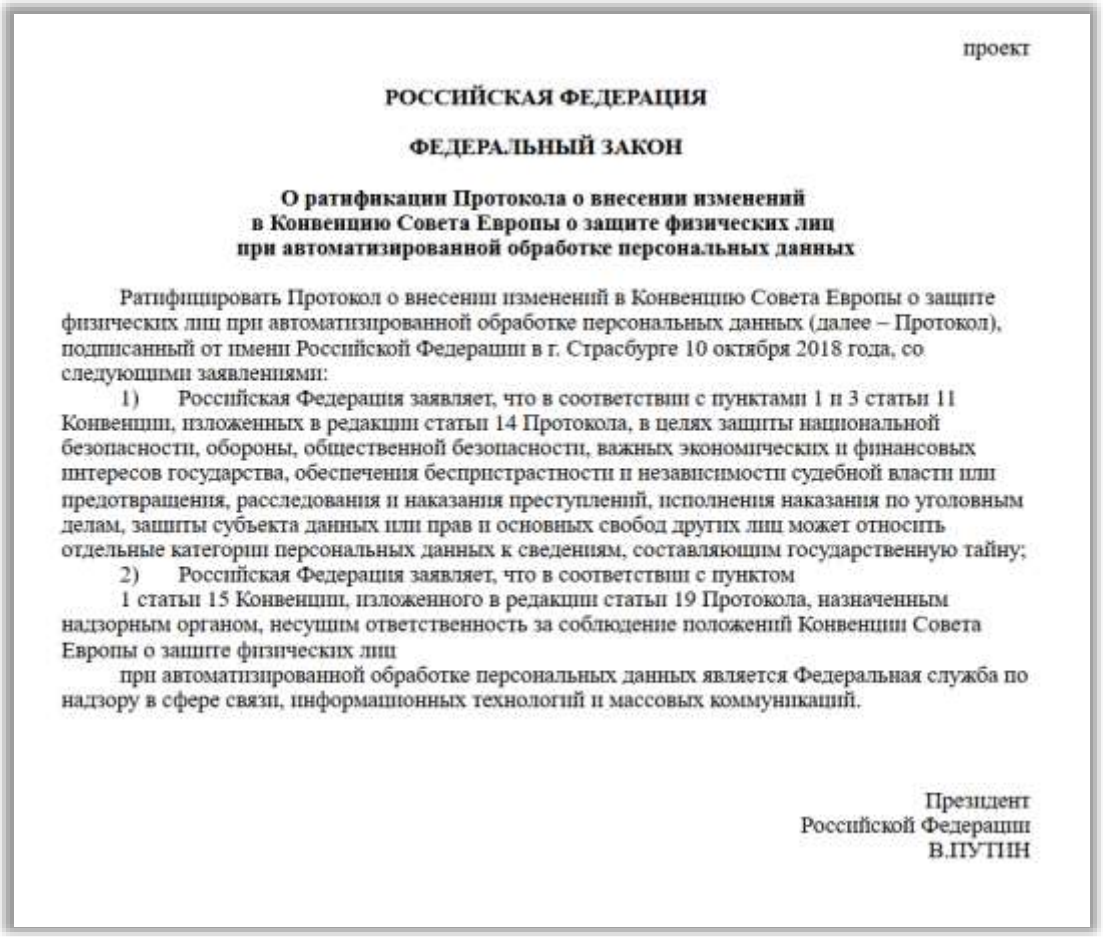
1. Требования к принципам пропорциональности, минимизации и законности сбора, обработки и хранения персональных данных. Эти принципы уже содержатся в ст. 5 Федерального закона «О персональных данных».

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.

https://rkn.gov.ru/news/rsoc/news62380.htm

308 Законопроект о ратификации РФ протокола СДСЕ № 223 к Конвенции 108



проект

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О ратификации Протокола о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных

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

1) Российская Федерация заявляет, что в соответствии с пунктами 1 и 3 статьи 11 Конвенции, изложенных в редакции статьи 14 Протокола, в целях защиты национальной безопасности, обороны, общественной безопасности, важных экономических и финансовых интересов государства, обеспечения беспристрастности и независимости судебной власти или предотвращения, расследования и наказания преступлений, исполнения наказания по уголовным делам, защиты субъекта данных или прав и основных свобод других лиц может относить 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».

https://regulation.gov.ru/projects#npa=95055

Отличия в защите персональных данных между GDPR и законодательством некоторых стран СНГ

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	✓	!	✗	✗	✗	!

Благодарю за ваше внимание



Алексей Мунтян

Эксперт по защите персональных данных и IT-безопасности

+7 (903) 762-64-15

muntyan.alexey@gmail.com

facebook.com/alexey.muntyan

linkedin.com/in/alexey-muntyan