General Data Protection Regulation

Практика реализации норм GDPR и реакция заинтересованных лиц

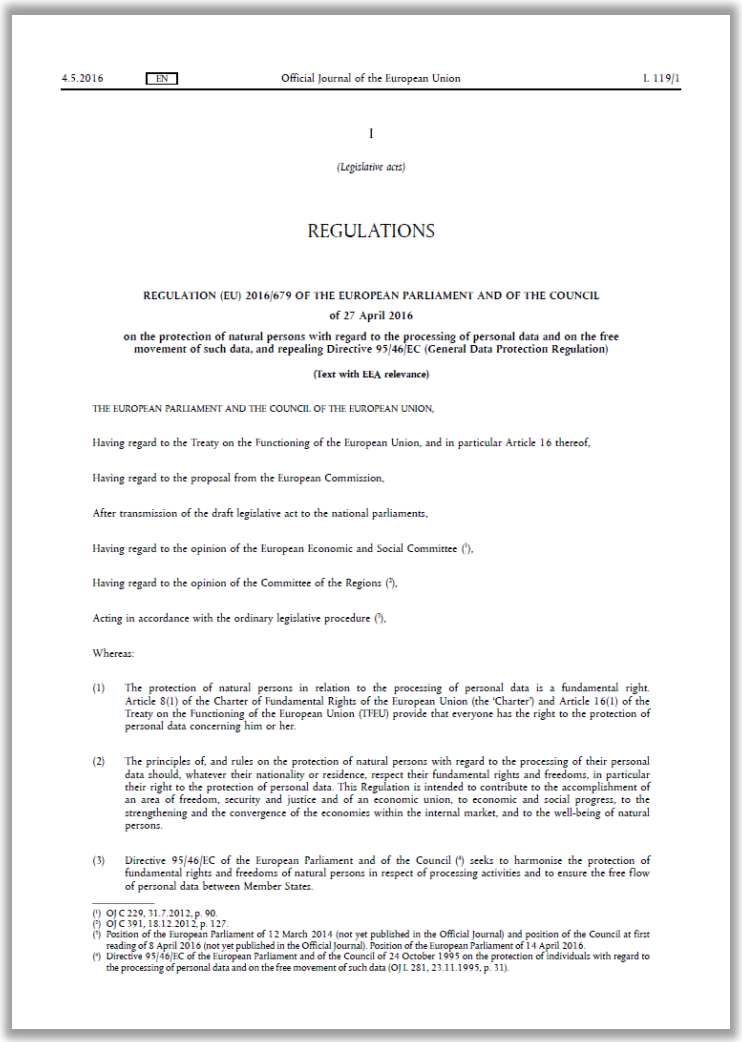
Алексей Мунтян
Эксперт по защите персональных данных и IT-безопасности

2 Об отношении к предмету обсуждения

© marketoonist.com

Эволюция европейского законодательства о защите данных

4 Что такое GDPR?



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.

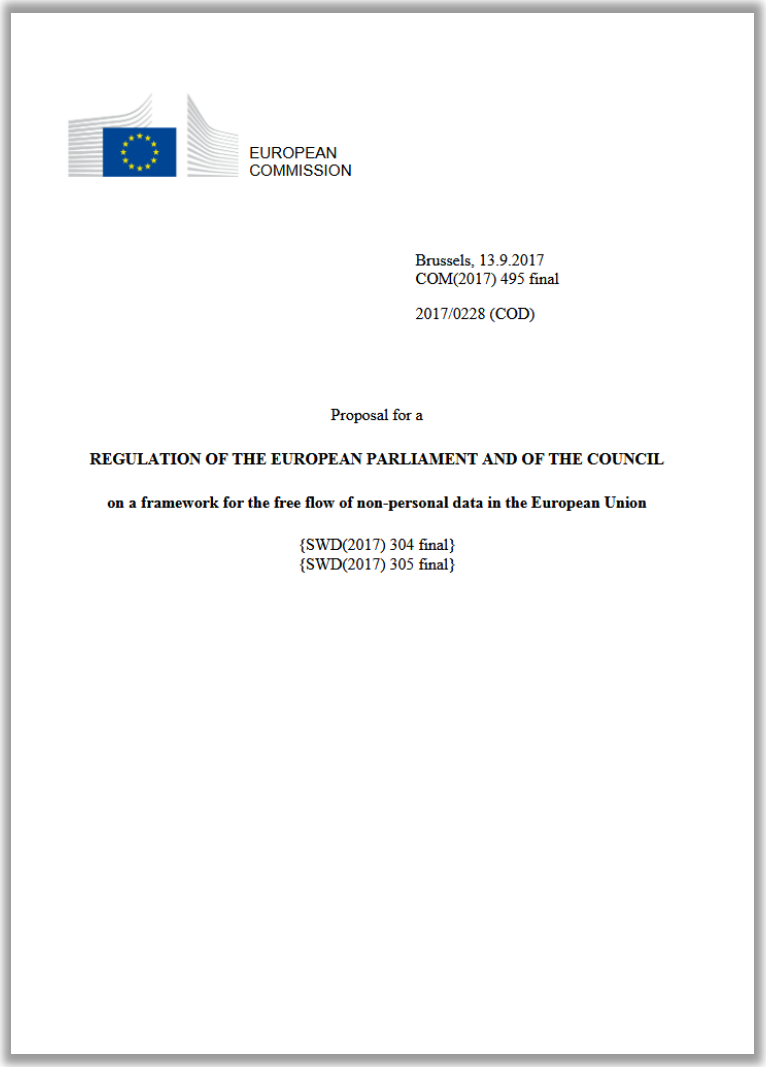
([1]) OJ C 229, 31.7.2012, p. 90.
([2]) OJ C 391, 18.12.2012, p. 127.
([3]) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European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

General Data Protection Regulation (GDPR) – это новый регламент ЕС о защите персональных данных, формирующий обязательные к соблюдению единые принципы и подходы как для государств-членов ЕС, так и для иных государств. 19.04.2018 проведена гармонизация прочтения некоторых положений GDPR на разных языках ЕС.

Некоторые факты:

- вступил в силу 25.05.2018
- заменяет собой Директиву 95/46/ЕС от 24.10.1995
- гармонизирует правотворчество и правоприменение
- локальный надзор осуществляется национальными органами стран-участниц Евросоюза по защите данных (Data Protection Authorities)
- общий надзор осуществляется Европейским советом по защите данных (European Data Protection Board)
- непосредственно применяется национальными судами государств-членов ЕС и Судом справедливости Евросоюза (European Court of Justice)

Digital Single Market: свободное перемещение в ЕС данных, не являющихся персональными



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:

- Framework for the free flow of non-personal data in the EU
- EU negotiators reach a political agreement on free flow of non-personal data

Примеры требований 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.

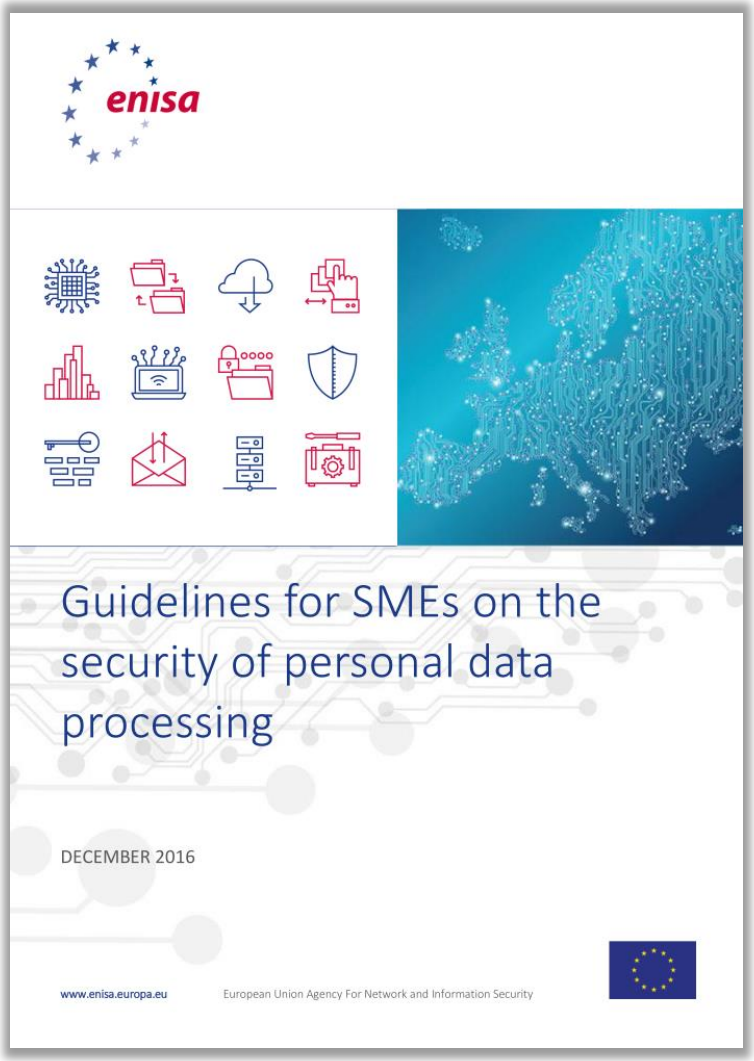
Руководство по европейскому законодательству о защите данных от FRA

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
EDPS

fra.europa.eu

Руководство для SME по защите персональных данных от ENISA

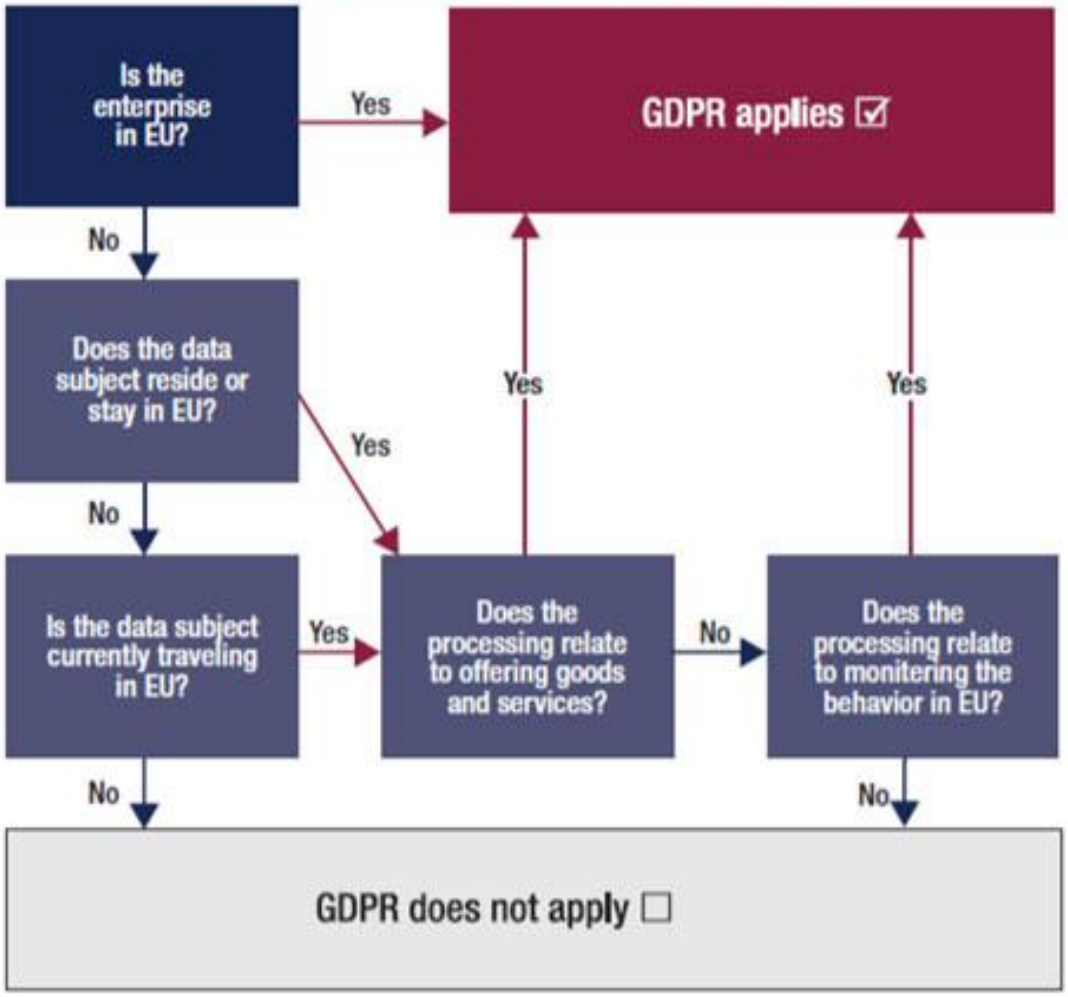


Security risk management for personal data

www.enisa.europa.eu

8 Сфера действия GDPR по версии ISACA

Figure 44—Determining If GDPR Applies to an Enterprise



Source: Varankevich, Siarhei; "Territorial scope of the GDPR (Flowchart)," LinkedIn, 17 February 2017, *www.linkedin.com/pulse/territorial-scope-gdpr-flowchart-siarhei-varankevich*, adapted per creative commons license at *https://creativecommons.org/licenses/by-sa/4.0/*

9 Сфера действия GDPR по версии Роскомнадзора

Требования Регламента Европейского союза по защите персональных данных не будут распространяться на российских операторов, работающих в России – А. Жаров

9 ноября 2017 года

Требования вст
Европейского с
будут распрост
осуществляющ
них распростра
сфере. Об этом
Александр Жар
VIII Междунаро,
данных».

По его словам,
участницей мех
устанавливающих порядок обработки персональных данных г
«Регламент, по нашему мнению, должен учитываться только п
европейских граждан российскими операторами на территори
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

rkn.gov.ru/news/rsoc/news51780.htm

rkn.gov.ru/news/rsoc/news53394.htm

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

20 декабря 2017 года

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.

Американский бизнес и GDPR

Business World

US companies block 500 million Europeans rather than deal with GDPR

Tom Maguire
May 27 2018 6:00 PM

https://www.independent.ie

F or some of America's biggest newspapers and online services, it's easier billion people from accessing your product than comply with Europe's ne Data Protection Regulation (GDPR).

The Los Angeles Times, the Chicago Tribune, and The New York Daily Ne

The Washington Post
Democracy Dies in Darkness

Europe, not the U.S., is now the most powerful regulator of Silicon Valley

https://www.washingtonpost.com

Europe implemented a sweeping overhaul of digital-privacy laws on Friday that has reshaped how technology companies handle customer data, creating a de-facto global standard that gives Americans new protections and the nation's technology companies new headaches.

These major changes underscored the extent to which the European Union has emerged as the most powerful regulator of Silicon Valley, stepping in where Washington has failed — or simply been unwilling — to limit some of the United States' most lucrative and politically influential companies.

The suite of new laws, collectively known as GDPR, for General Data Protection Regulation, gives users the right to demand the deletion of data and object to new forms of data collection while requiring that companies get explicit consent for how they collect, process and use data — practices that had been all but unfettered in the United States. Potential violators could face fines of up to 4 percent of global profits.

The Guardian

bal development Football **Tech** Business Environment Obituaries

https://www.theguardian.com

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.

CNBC

Search Quotes, News & Video

Facebook, Google face complaints worth $8 billion over alleged breach of new EU data law

https://www.cnbc.com

- Max Schrems' non-profit organization NOYB filed complaints against Google, Facebook and Facebook-owned services WhatsApp and Instagram.
- Schrems alleged that the companies "forced consent" from users to obtain the right to use their data and comply with the EU's GDPR.
- Schrems accused Facebook and Google of not giving users a "free choice" to agree to the tech firms using their data.

11 Российский бизнес и GDPR

3DNews ••• Новости Software ••• Шутер ••• Серверы Super Monday Night Combat отключ...

Новости Software

Серверы Super Monday Night Combat отключат из-за новых законов ЕС о конфиденциальности

30.04.2018 [14:51], Алексей Лихачев https://3dnews.ru

Условно-бесплатная MOBA Super Monday Night Combat прекратит своё существование в следующем месяце из-за новых законов о конфиденциальности ЕС. Игра уже исчезла из магазина Steam, а у обладающих ею пользователей она перестанет запускаться 24 мая.

Общий регламент по защите данных (GDPR) направлен на то, чтобы гарантировать безопасность пользователей и заставить компании соблюдать требования по обработке и хранению данных. Тех, кто к 25 мая не изменит инфраструктуру в соответствии с законом, ждут огромные штрафы.

Как сообщили в беседе с Polygon разработчики из Uber Entertainment, в нынешнем виде мультиплеерная составляющая не соответствует требованиям GDPR. А на её переделывание уйдёт значительно больше денег, чем было потрачено на создание проекта. В качестве

Новый регламент ЕС по защите персональных данных вынуждает компании отказываться от европейского трафика

https://servernews.ru

28.05.2018 [09:59], Андрей Крупин

евросоюз

защита данных

информационная безопасность

сети

Рекламно-технологическая группа «ОТМ» приняла решение о переводе серверных мощностей с европейских на российские площадки. Таким образом компания намерена минимизировать риски, связанные с вступлением в силу в Евросоюзе «Общего регламента по защите данных» (англ. General Data Protection Regulation, GDPR), ужесточающего правила работы с персональными данными интернет-пользователей. До сих пор компания арендовала более 30 серверов в нескольких дата-центрах Германии и Франции. Перевод приведёт к заметному росту стоимости серверных мощностей для «ОТМ»: ежемесячные арендные платежи вырастут на 20%.

Регламент GDPR был принят в апреле 2016 года и вступил в силу 25 мая после двухлетнего переходного периода. Авторы документа утверждают, что он призван дать гражданам ЕС контроль над своими персональными данными, унифицировать защиту этих данных и их экспорт из Евросоюза. Несоблюдение требований закона грозит нарушителям, в том числе из стран, не входящих в Евросоюз, крупными штрафами: максимально до 20 млн евро или до 4% от суммарного годового оборота компании.

Плохие ребята и GDPR

HackRead

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

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

Ransomhack; a new attack blackmailing business owners using GDPR

By Waqas on June 23, 2018 Email @hackread CYBER CRIME HACKING NEWS

Hackers Are Threatening Companies To Leak Stolen User Data Online To Hurt Them Through GDPR Regulations – In Return They Are Demanding Ransom Money.

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

Взломав серверы очередной жертвы и похитив персональную информацию, преступники не планируют её как-либо использовать, а лишь угрожают публикацией. В соответствии с GDPR компанию ждет крупный штраф в случае утечки, поэтому, чтобы не попасть под санкции Европейского Союза, организации предпочитают выполнить требования злоумышленников.

hackread.com

Европейский суд об определении контроллера данных

Press and Information

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

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
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

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

curia.europa.eu

14 Бонусный слайд: CPA and PDPA

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

There is a strict local Data Protection regulation in Russia, which could prevent the Russian legal entity from straight following global and regional requirements with respect to signing the Controller-to-Processor Agreement (CPA). In that case it is proposed to conclude a Personal Data Protection Agreement (PDPA) between the Russian legal entity and the European one instead of CPA, which:

- ✓ establishes the principle of equality parties, does not give any advantages to either party and does not infringe the interests of both parties;
- ✓ establishes a legal framework and regulates all contractual relations between parties regarding processing and protection of personal data;
- ✓ protects the rights and legitimate interests of personal data subjects;
- ✓ reduces the risk of claims from relevant Data Protection Authorities;
- ✓ allows both parties to engage (assign) third parties to the processing of personal data.

Алексей Мунтян
Эксперт по защите персональных данных и IT-безопасности
+7 (903) 762-64-15
muntyan.alexey@gmail.com
www.facebook.com/alexey.muntyan

Благодарю за внимание