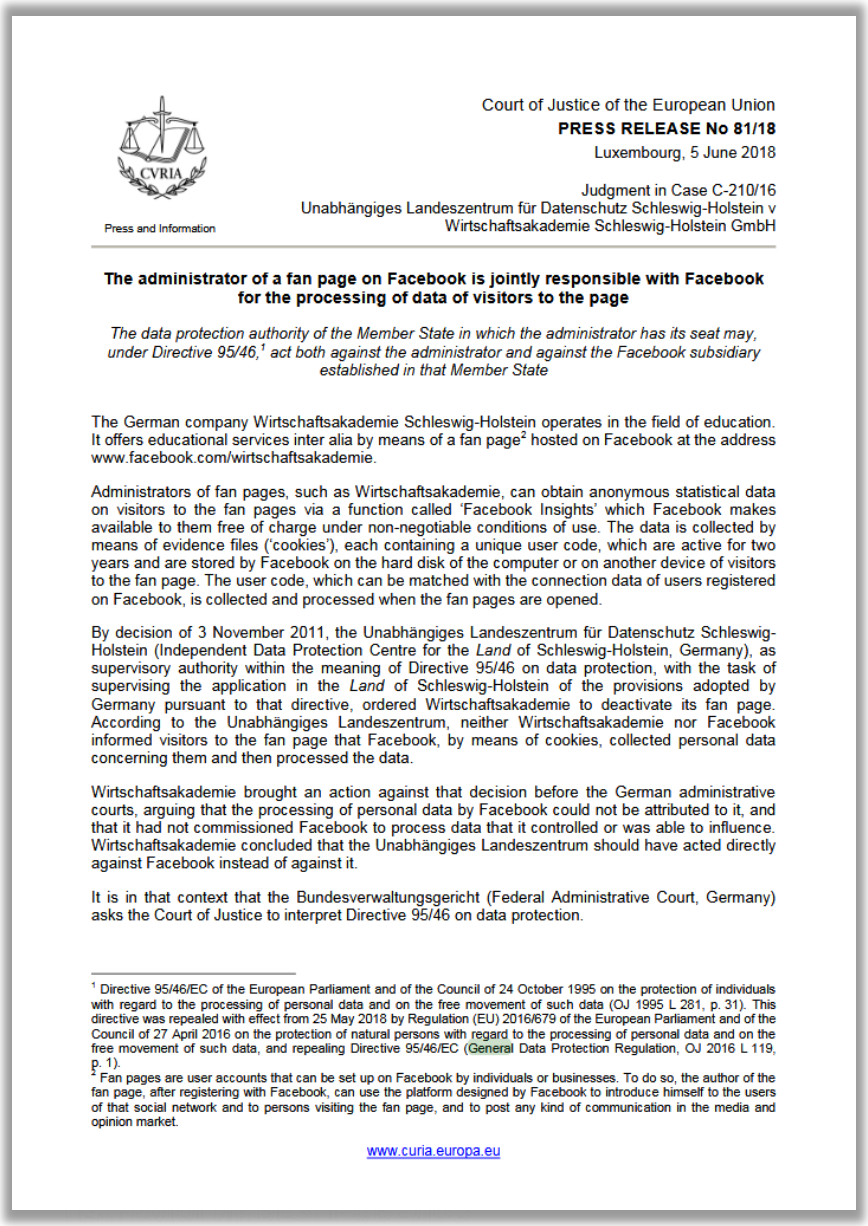
General Data Protection Regulation

Жаркое лето 2018 года:
практика компланеса GDPR

Алексей Мунтян
Эксперт по защите персональных данных и
IT-безопасности

2 Европейский суд об определении контроллера данных



Court of Justice of the European Union
PRESS RELEASE No 81/18
Luxembourg, 5 June 2018

Press and Information

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

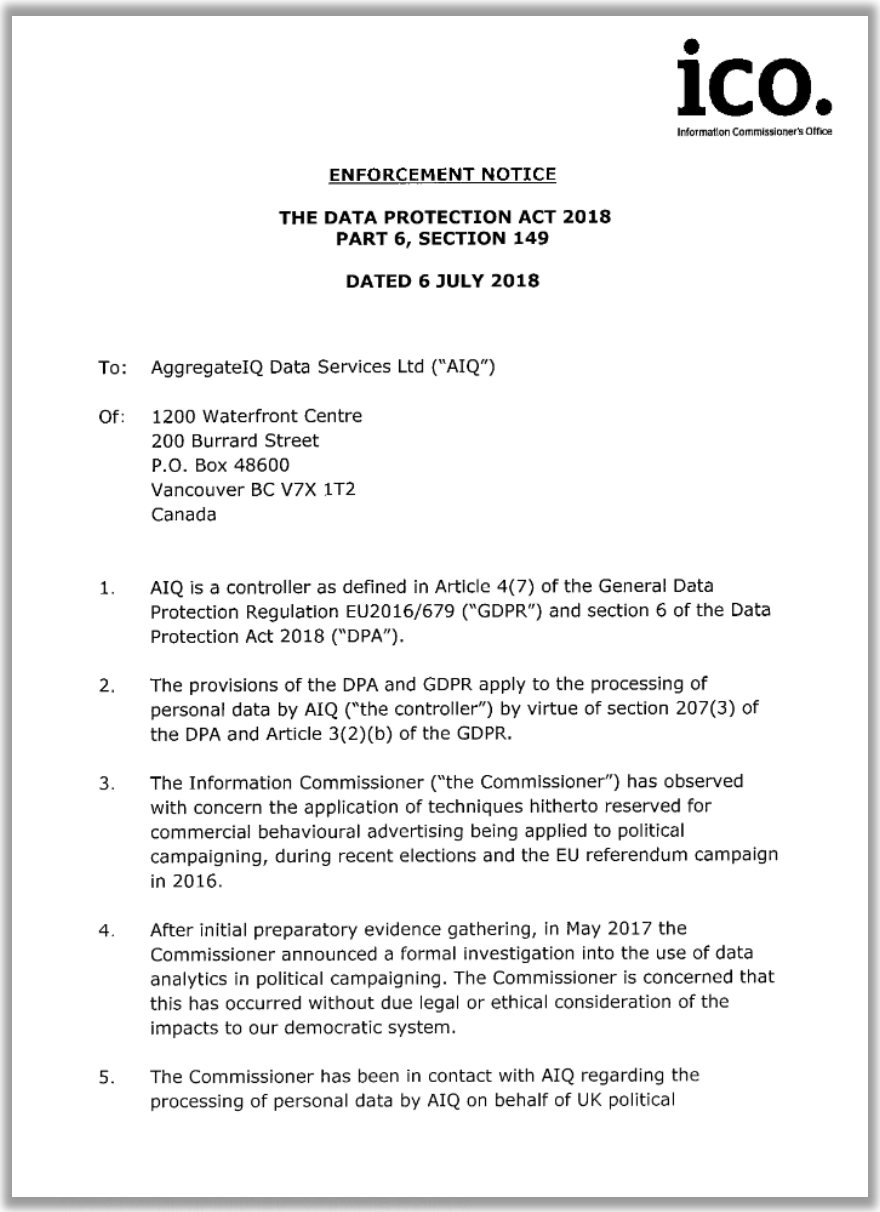
Court of Justice of the European Union
PRESS RELEASE No 81/18
Luxembourg, 5 June 2018

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

3 Практика GDPR: предписание о прекращении обработки



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.

ico.org.uk

4 Практика GDPR: первый штраф

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.

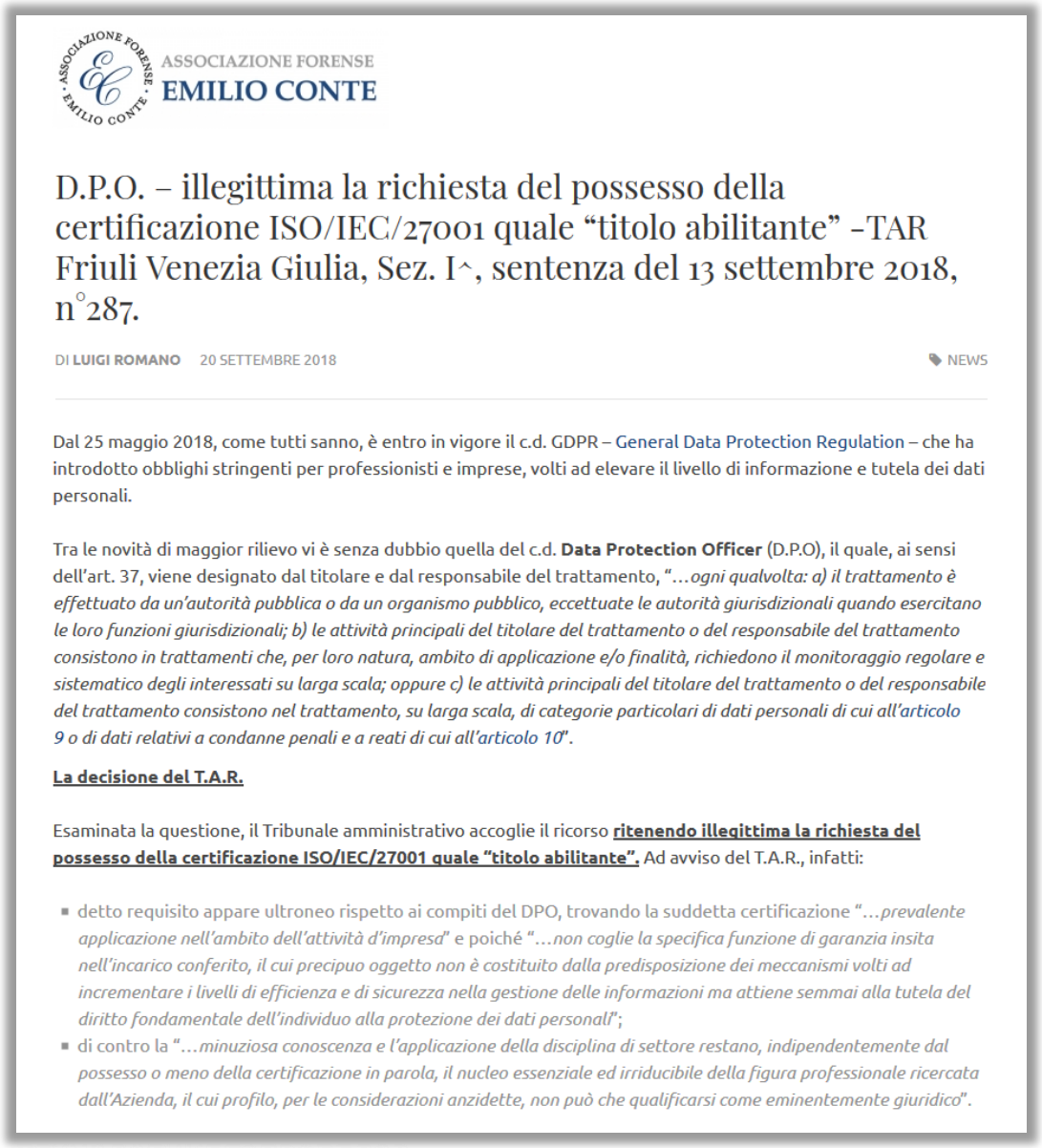
Es betrifft das Reisebüro ums Eck genauso wie die Netzgiganten Facebook oder Google: Die Datenschutz-Grundverordnung (DSGVO) gibt EU-Bürgern seit Ende Mai mehr Mitsprache dabei, was Unternehmen mit ihren persönlichen Daten machen. Bei Verstößen sind Strafen von bis zu 20 Millionen Euro oder bis zu vier Prozent des Konzernumsatzes möglich.

Salzburger Nachrichten:

Первый штраф за нарушение GDPR в Австрии составил 4800 евро за неправильно настроенную систему внутреннего видеонаблюдения (CCTV).

www.sn.at

5 Практика GDPR: требования 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.

associazioneforenseemilioconte.it

6 Практика GDPR: 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.

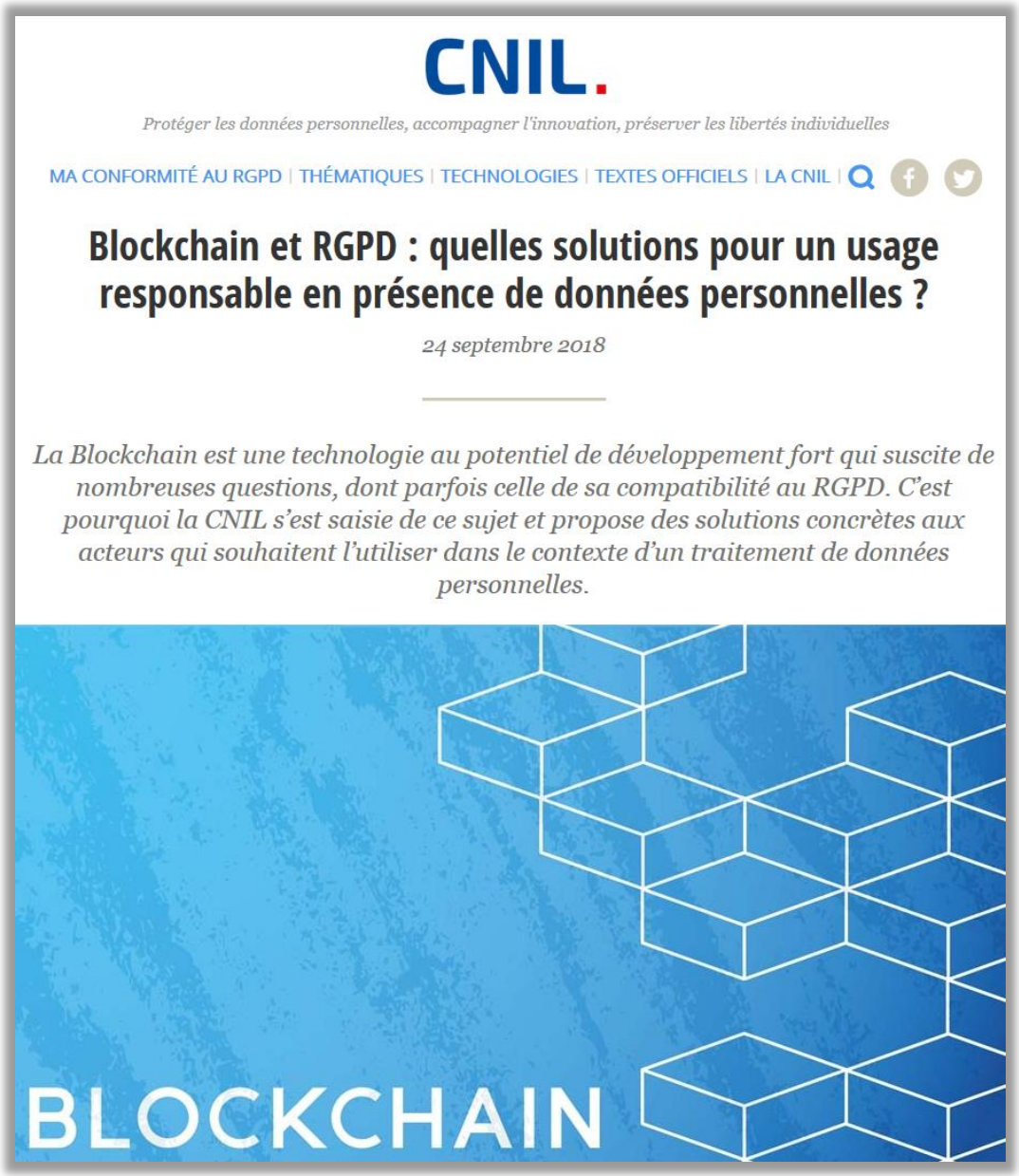
It comes as a new European data privacy law, the General Data Protection Regulation (GDPR), puts a premium on access to customer data given by consent, structurally favoring direct marketing channels over the advertising ecosystem that relies heavily on tracking users online.

The Thomson Reuters:

SAP, Microsoft и Adobe создали альянс «Open Data Initiative» для выполнения требования GDPR о переносимости персональных данных.

www.reuters.com

7 Практика GDPR: использование технологии блокчейн

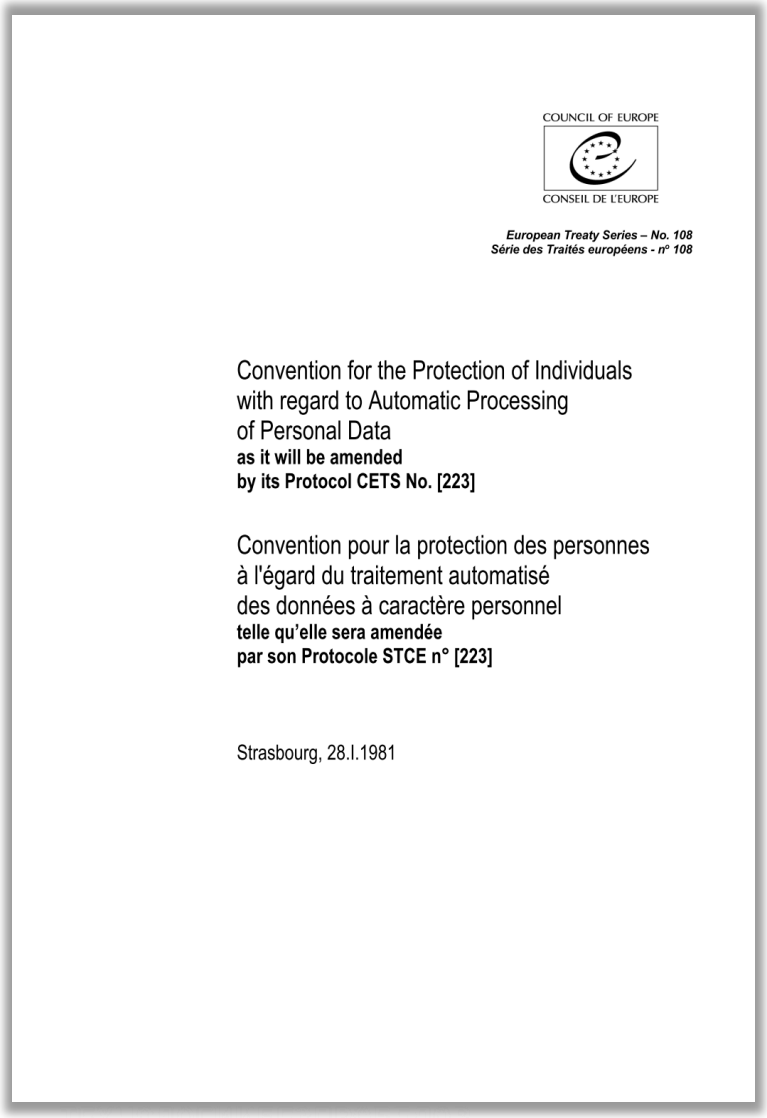


Commission nationale de l'informatique et des libertés:

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

www.cnil.fr

8 Внесение изменений в Конвенцию ETS № 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, в том числе, и в сфере гармонизации многих положений Конвенции с нормами GDPR (например, использование в Конвенции понятий controller, processor, recipient, использование концептов privacy by design, privacy by default, privacy impact assessment и т.д.). Протокол будет открыт для подписания в Страсбурге 10.10.2018 в ходе четвертой части сессии Парламентской ассамблеи Совета Европы.

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

Новая редакция Конвенции и РФ:

- принятие Россией Протокола потребует от нее как возвращение к работе в рамках ПАСЕ и уплаты взносов в Совет Европы, так и издания правовых актов, имплементирующих положения новой редакции Конвенции в национальную систему регулирования обработки и защиты персональных данных;
- расширение статуса и полномочий Комитета Конвенции с консультативных до исполнительных и надзорных (статьи 22-24 новой редакции Конвенции) может вызвать у российских властей определенные сомнения в целесообразности принятия Протокола.

9 США готовят свой 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.

www.ntia.doc.gov

10 Определение сферы действия GDPR

[1] **ЕС** – территория государств-членов Европейского союза, **ЕАСТ** – территория таких государств-членов Европейской ассоциации свободной торговли как Исландия, Лихтенштейн, Норвегия.

[2] Основным квалифицирующим признаком является поручение обработки таких персональных данных, которые были получены у субъекта в момент его нахождения на территории ЕС/ЕАСТ. Кроме того, существенное значение для квалификации поручения обработки персональных данных имеет способ оформления такого поручения. Например, поручение обработки персональных данных субъектов, находящихся на территории РФ, оформленное в виде Controller-to-Processor Agreement с учетом требований и механизмов GDPR между российской и европейской организациями существенно повышает риск того, что оно будет рассматриваться в ЕС/ЕАСТ как подпадающее под регулирование GDPR.

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-26369a36

Благодарю за внимание