Deloitte.

Belgium | Audit & Enterprise Risk Services | October 2015

Privacy Flash
Privacy at your fingertips

Privacy is becoming increasingly important to everyday business. Legal developments and regulators' increasing attention to privacy are two of the key drivers behind this. The aim of the "Privacy Flash" series is to bring to an audience eager to learning more about privacy, selected information on regulation, awareness events and initiatives related to personal data protection, as well as indicative privacy-related topics and current projects taking place.

You can find our previous issues on our website.

We hope that you will find this bi-monthly newsletter interesting. For additional information or suggestions on how to improve the "Privacy Flash", or to (no longer) receive the next issue directly via email, please send an email to BEPrivacyFlash@deloitte.com.

Issue 7
October 2015

Breaking

EU’s highest court declares Safe Harbor invalid

The Court of Justice of the European Union (CJEU) has ruled on October 6, 2015 that the EU-US Safe Harbor Framework for transferring personal data from the EU to the US is invalid.

Background

The case was brought before the EU’s highest court by Max Schrems, an Austrian Facebook user who lodged a complaint with the Irish Data Protection Authority (DPA) after the Snowden revelations had shown that his data and that of other EU citizens had been accessed by US intelligence services. Data from European Facebook users is transferred from its subsidiary in Ireland to servers located in the US, where it is processed. The Irish DPA first rejected the complaint on the grounds that, under the Safe Harbor scheme, the United States had been deemed by the European Commission to ensure an adequate level of protection of transferred personal data (i.e. protection equal to EU standards).

The High Court of Ireland, to which the case was then brought, asked the CJEU whether this reasoning holds, i.e. whether the existence of a decision from the European Commission (the EU’s executive body) establishing that a third country ensures an adequate level of protection can eliminate or reduce the powers available to a national DPA to examine whether this is indeed the case. The CJEU clearly rejected this reasoning and argued that **a national DPA must be able to examine, with complete independence, whether the transfer of a person’s data to a non-EU country complies with the requirements laid down by the EU Data Protection Directive.**

The CJEU further confirmed that it alone can declare a European Commission Decision invalid, and therefore went on to investigate the adequateness of the Safe Harbor framework. **The Court of Justice of the European Union decided to declare the Safe Harbor Decision invalid** for the following reasons:

- National security, public interest and law enforcement requirements of the United States prevail over the Safe Harbor scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by the scheme where they conflict with such requirements;
- United States authorities were able to access the personal data transferred from the EU to the United States and process it in a way incompatible with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security;
- The persons concerned had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

The CJEU only declared it invalid. It did not foresee any grace period or transition period.

Consequences: Revising data transfer strategy

The direct consequence of this ruling is that **the Irish DPA** will now have to examine Max Schrems' complaint with due diligence, and at the conclusion of its investigation, **is to decide whether, pursuant to the Directive, the transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data**.

A much wider consequence of the CJEU ruling is that one of the most important and most used legal frameworks for transfers of personal data between the EU and the US has been declared invalid, forcing 4,400 US-based companies to revise their data transfer strategy in the short term.

The European Commission confirmed in a press conference later in the day that other mechanisms for organising data transfers to the US, such as EU model contracts, binding corporate rules (BCRs; for intra-group transfers) remain valid. In addition, it emphasised that the Data Protection Directive includes certain derogations that allow for international data transfers, i.e. when necessary for the performance of a contract (e.g. EU citizen booking a hotel in the US), on important public interest grounds (fight against fraud, etc.), to protect a vital interest of the data subject (emergency situations), or based on the free and informed consent of the data subject.

Next steps

The Commission will shortly issue guidance to national DPAs and businesses in order to ensure a uniform interpretation of the ruling across the EU, reinstate legal certainty for businesses and safeguard the transatlantic flow of data – calling it "the backbone of the European economy". To this end, it will cooperate with the Article 29 Working Party, the EU's advisory body on data protection which brings together all 28 national DPAs. In addition, the Commission will act as a point of contact for queries from organisations.

In the meantime, the European Commission will continue the negotiations with the US on a new Safe Harbor Framework that started in October 2013. Commissioner Věra Jourová noted that the CJEU ruling acknowledges the concerns that were raised by the Commission in 2013, and that the negotiations will build on the ruling going forward. She could not state a deadline for the negotiations at this time, as the negotiations on national security aspects are taking more time than she had initially hoped.

As a side note, the Commissioners said that the negotiations on the reform of the EU data protection legislation, in the form of the **General Data Protection Regulation, is still scheduled to end by the end of 2015**.

We will keep our ears to the ground on the impact of the Safe Harbor CJEU decision and the reactions per country, on the ongoing negotiations between the EU and the USA for an updated 'safer' Safe Harbor agreement, and on the EU negotiations on the General Data Protection Regulation.

Further information:

- The official CJEU press release
- The official CJEU judgement
- The European Commission press conference of 6 October 2015 (video):
  - http://ec.europa.eu/avservices/video/player.cfm?ref=I109752
  - http://ec.europa.eu/avservices/video/player.cfm?ref=I109753
  - http://ec.europa.eu/avservices/video/player.cfm?ref=I109754

News

ICO issues its largest ever fine for nuisance calls

The Information Commissioner's Office (ICO), the UK Data Protection Authority, has ruled that Home Energy & Lifestyle Management Ltd (HELM), a green energy company, has recklessly broken marketing call regulations, and issued a fine of £200,000, the ICO's largest ever in relation to nuisance calls.

The ICO discovered that HELM used an automated calling system to make over six million direct marketing calls to offer British consumers 'free' solar panels. The system was not set up in a compliant manner as the calls were often repeated and it was not always possible to connect to a person or to stop the calls by pressing an option button. And most importantly, a key requirement for making direct marketing calls using an automated calling system is to obtain a person's specific consent to receiving automated calls. The company admitted it was not aware of the rules. The record fine should be seen as a warning to other firms, according to ICO Head of Enforcement Steve Eckersley.

The ICO's detailed guidance on carrying out direct marketing activities explains the legal requirements under the Data Protection Act (DPA) and the Privacy and Electronic Communications Regulations (PECR).

US Department of Defense now requires contractors to report more cyber incidents

The U.S. Department of Defense (DoD) announced on October 2nd that it will soon require all of its contractors to report any cyber incidents that result in an actual or potential adverse effect on their systems or defence information residing therein, or on a contractor's ability to provide operationally critical support. The decision was taken after several incidents relating to US government officials and their personal data, including the data breach of 22 million government personnel's sensitive information, including security clearances and 5.6 million sets of fingerprints.

Until now, contractors used a voluntary system to report serious breaches of various kinds, but were already required to report breaches of personally identifiable information or financial information. The new directive will broaden the mandatory reporting.

Recent breaches and enforcement actions

- On 15 September 2015, Experian, a credit agency data broker, has discovered an unauthorised party accessed T-Mobile data housed in an Experian server. Experian published a statement on its website to explain the incident, what it is doing to resolve it and how affected persons can take action.
- On September 21st, the CNIL, the French data protection authority, rejected Google's informal appeal to an order of the CNIL that requires Google to block French results removed from all of Google's sites (in addition to google.fr), after a request to remove internet search results under the EU “right to delisting”.
- On October 1st, Scottrade Inc., a retail brokerage firm disclosed a breach involving contact information and possibly Social Security numbers on 4.6 million customers. The breach appears to have occurred over a period between late 2013 and early 2014. Scottrade said it would contact all affected individuals with additional information and resources.

Forthcoming interesting events

14th Annual Data Protection Compliance Conference

London, UK, 15-16 October 2015
http://www.pdpconferences.com/find-a-conference/82-14th-annual-data-protection-compliance-conference

A 2-day Data Protection Conference held in Central London specifically designed to give Information Professionals the key resources and practical information they need in their daily work.

37th International Privacy Conference

Amsterdam, NL, 26-29 October 2015
https://www.privacyconference2015.org/

The International Privacy Conference is the assembly of all accredited data protection and privacy commissioners from around the world and will be hosted this year by CBP, the Dutch Data Protection Authority. During the conference, the results of the Privacy Bridges Project will be presented. This project was launched in April 2014 on the initiative of Jacob Kohnstamm, the chairman of the Dutch DPA and aims at finding common ground between US and EU approaches to privacy.

European Privacy Academy

http://www.europeanprivacyacademy.com/

The European Privacy Academy is a unique training, knowledge and networking centre focused on the actual day-to-day management of the privacy challenge. It provides both an on-campus data protection officer course and on-campus or in-house department-specific data protection trainings during which attendees learn to efficiently manage privacy and security in a risk based and integrated manner.

The next sessions of the European Privacy Academy are listed below:

DPO Course – January 2016: 18 – 21 January 2016 & 15 April 2016

IAPP Europe Data Protection Congress

Brussels, BE, 30 November – 3 December
https://iapp.org/conference/iapp-europe-data-protection-congress-2015/

Training and workshops: 30 November – 1 December 2015
Conference: 2-3 December 2015

Homepage

Deloitte Belgium
Berkenlaan 8A, 8B, 8C
1831 Diegem
Belgium