Deloitte.

July 2016

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 is to provide monthly updates on global regulatory developments, as well as relevant news and information on upcoming events in the field of data protection and privacy.

Previous issues are available on our website.

For additional information, improvement suggestions for our Privacy Flash, to subscribe or unsubscribe, please contact us via email: deloitte.ch.news@deloitte.ch

Issue 6, July 2016 Highlights

EU-US Privacy

Privacy Shield adopted

On 12 July 2016, the European Commission adopted the EU-US Privacy Shield framework with an adequacy decision. By notifying the Member States, the new framework for EU-US personal data transfers enters into force immediately. The adoption of the Privacy Shield signals a return to normality for transatlantic data transfers, after the previous Safe Harbour framework got invalidated by the European Court of Justice in October 2015.

As of **1 August 2016**, companies will be able to self-certify with the US Department of Commerce operating the shield.

Key Elements

A draft version of the Privacy Shield adequacy decision presented by the European Commission in February 2016 elicited comments from the Article 29 Working Party and the European Data Protection Supervisor (EDPS), which requested additional clarifications and improvements, in particular with regards to data retention, onward transfers and redress mechanisms for EU data subjects (see also Privacy Flash issue 4).

Following these comments, the European Commission and the US Department of Commerce renegotiated the deal in the past few months. The final deal reached was approved on Friday 8 July by the Article 31 committee which represents the EU Member States, and contains the following main elements:

- **Obligations on companies**: Companies will be able to self-certify with the US Department of Commerce by committing to comply with the Privacy Shield Principles. This entails amongst others that companies must provide effective redress mechanisms to deal with data subject complaints, that employees receive training about their obligations under internal privacy policies, and that compliance is periodically reviewed. Participating organisations will have to re-certify every year and ensure that any onward transfers of personal data are covered by a contract with the receiving third party that provides the same level of protection.
- **Enforcement**: The US Department of Commerce will conduct regular updates and reviews of participating companies. Companies found to be non-compliant can face sanctions and be removed from the list.
- **Protection of data subject rights**: Citizens will have several ways to issue complaints about the use of their personal data by Privacy Shield organisations. In a first instance, complaints should be handled by the company itself, but free of charge. Alternative Dispute Resolutions (ADR) will be offered if the company does not deal with it. In addition, data subjects can direct their concerns to national Data Protection Authorities, who will liaise directly with the Federal Trade Commission to ensure that issues are investigated and resolved. As a last resort, there will be an arbitration mechanism. Redress in the area of national security will be handled by an Ombudsperson independent from the US intelligence services.

- **Safeguards related to US government access**: The **US has given the EU assurance** that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms. In addition, the Commission reported that the US has ruled out indiscriminate mass surveillance on personal data transferred to the US under the EU-US Privacy Shield arrangement.

Links

- European Commission press release
- EU-US Privacy Shield adequacy decision
- US Department of Commerce factsheet

Hamburg DPA fines three companies over Safe Harbour

Over the course of the last few months, the Data Protection Authority (DPA) of Hamburg has fined three companies that were still relying on the EU-US Safe Harbour framework six months after its invalidation by the European Court of Justice. The three companies concerned had not switched fast enough to alternative transfer methods such as standard contractual clauses.

In theory, each fine could have amounted to up to 300,000 euro. The companies were however only fined between 8,000 and 11,000 euro, as they had eventually put standard contractual clauses in place. The decision served to highlight the need for companies to find an alternative legal safeguard to cover their data transfers to the US, with the Hamburg DPA warning that other companies may be fined in the near future as well.

News

Brexit creates questions over privacy rules

On 23 June 2016, the UK held a referendum to decide whether or not to remain a member of the European Union, which resulted in a win for the "Leave" camp. The referendum is not legally binding for the British government. However, since most people consider it politically binding it is therefore more than likely that the UK will leave the European Union in the course of the next few years.

If the UK were to leave the European Union, it would most likely put in place a legal framework that reflects the provisions of the GDPR. In order for the UK to continue to trade with the EU and Switzerland on equal terms, the UK Information Commissioner's Office (ICO) confirmed that it would seek recognition as an adequate jurisdiction. This would entail that the UK, similar to the Swiss model, would adopt data protection standards equivalent to the GDPR, which would allow for a continued free flow of personal data between the EU and the UK.

Much will depend on the model the UK and the rest of the EU negotiate for UK's relationship with the remaining EU member states. Should the UK decide to exit the EU, it needs to follow the formal legal procedure set out in Article 50 of the Treaty of the European Union. This procedure takes a minimum of two years, which means that companies still need to prepare for the entry into force of the GDPR on 25 May 2018.

From a Swiss – UK data protection perspective, there is no need for any rushed decisions. The GDPR will officially come into force 28 May 2018, and thus apply in the UK prior to the formal exit from the European Union. There are some concerns that an eventual "Brexit" might disrupt the data flow for international businesses. Special instruments for Swiss and other third country transfers may need to be introduced as mitigating measures with regard to data transfers in and from the UK. For cloud, digital or finance-based services in Switzerland that use a variety of providers in the UK, this might result in a substantial need for adjustments of their processes and contractual arrangements. Companies may, for example, consider to focus on Brexit through the definition of standard contractual clauses, binding corporate rules or the choice of service providers within an EU member state.

Revision of Swiss Federal Data Protection Act ("FDPA")

The pending revision of the Swiss data protection law is expected to be ready for the consultation process by end of August 2016. While the core principles of the FDPA are expected to remain the same, and only minor adjustments of the current law are required, Swiss law makers may copy large parts of the final GDPR into the revised FDPA to maintain the adequacy and harmonisation with the EU member state standards. Should the revised draft also adopt the substantial administrative sanctions regime from the GDPR, the revised FDPA may create significant boardroom attention and increase internal compliance efforts.

Advocate General of the European Court of Justice issues opinion in Amazon case

In recent years, the European Court of Justice (ECJ) already ruled on the applicability of the Data Protection Directive 95/46/EC in the Google Spain Case and the Weltimmo Case. In both judgments the ECJ expanded the scope of applicability of the Privacy Directive: In the *Google Spain Case*, the ECJ judged that a company's activities conducted from outside the EU can still be subject to the Directive when 'closely linked' to the activities of an establishment in the EU. In *Weltimmo Case*, the ECJ broadened the concept of an 'establishment' by stating that an establishment, based on a factual determination, refers to any stable arrangement.

In the current Amazon case, the Court is to rule on the scope of applicability in the context of online sales. A consumer protection body has challenged the website terms of Amazon, which state that Luxembourg law applies to the sale of goods online. The plaintiff argues that Austrian instead of Luxembourg law must be applicable when goods are being sold to Austrian consumers.

On 2 June 2016, the Advocate General (AG) of the ECJ issued an opinion in this case (not yet available in English), stating that, per *Weltimmo*, the activities of Amazon EU seem to be carried out from Luxembourg, thus it is more likely that the privacy law of Luxembourg is applicable. The AG determined that the criteria set out in *Google Spain* are not applicable in this case, as it concerns a conflict of privacy laws.

It seems that the AG wants to put an end to the expansion of the application of EU privacy laws, or at least rationalise it.

The opinion is not binding for the ECJ, however, the ECJ tends to follow the opinion of the AG. The decision of the ECJ is expected in the coming months.

EDPS launches accountability initiative

The principle of accountability takes a central role in the General Data Protection Regulation (GDPR). It entails that data controllers and processors must be able to demonstrate compliance with the GDPR's various provisions at all times.

In this context, the European Data Protection Supervisor (EDPS) - the data protection authority for European institutions and bodies - developed a framework for greater accountability in data processing in 2015, which was implemented first at the EPDS institution internally. The framework consists of a questionnaire addressed to the Supervisors, the Director, the staff responsible for processing operations and the Data Protection Officer.

In order to develop awareness for the new obligations under the GDPR and their implications, the EDPS plans a series of visits this year to small, medium and large EU institutions. The EDPS will help companies to implement the accountability principle and share some of their practical tools.

Umbrella agreement on law enforcement cooperation

On 2 June 2016, the EU and U.S. signed the so-called "Umbrella agreement" on criminal law enforcement cooperation. It will improve the cooperation between EU and US law enforcement authorities by putting in place a comprehensive high-level data protection framework. This agreement is not a legal instrument in itself, however it is complementary to existing and future agreements between law enforcement authorities of the EU, its Member States and the US.

The Agreement includes data protection measures for data transfers for law enforcement purposes. In particular, it provides for an equal treatment of EU and US citizens with regard to judicial redress rights before US courts. Other safeguards that are included in the agreement concern the obligation to define appropriate retention periods and the obligation to seek prior consent before any onward transfer of data.

The European Parliament needs to give its consent before the European Council can adopt a final decision authorising the signing of the Umbrella agreement between the EU and US.

Bavarian DPA provides further guidance on GDPR

On 25 May 2018, the General Data Protection Regulation (GDPR) will enter into force. This means that there is a transition period of two years that allows companies to adapt to the new rules. In order to provide further guidance on the new data protection requirements, the Bavarian Data Protection Authority (DPA) will publish a short

paper in German twice a month on various topics covered by the GDPR.

On 10 June 2016, the DPA released its first paper discussing Article 32 of the GDPR concerning the security of processing.
Article 32 sets out the requirement for controllers and processors to implement appropriate technical and organisational measures while "*taking into account the state of the art and the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*". The GDPR, in comparison with the Directive, provides for specific security actions to be considered.

The second paper focuses on Article 42 GDPR, which recognises certifications as acceptable mechanisms for demonstrating compliance of the data processing activities with the requirements set out in the GDPR. According to the Bavarian DPA, certifications can be beneficial for companies as a mechanism to show the level of compliance of their data processing operations with the requirements set out in the GDPR.

Belgian DPA publishes 2015 annual report

On 9 June 2016, the Belgian Privacy Commission released its annual activity report for 2015. One of the main accomplishments of the Belgian DPA was the investigation of Facebook's terms of use, which resulted in a decision by Facebook to deny access to "public" Facebook pages for Belgians who are not a member of the social network. Furthermore, the DPA published a file on privacy issues in the workplace, issued various recommendations on the use of cookies and assessed the anti-terrorism measures proposed by the government. The 2015 annual report is available in Dutch and in French.

Irish DPA intends to challenge model clauses

In October 2015, the European Court of Justice (ECJ) ruled that the Safe Harbour Decision is invalid for transferring personal data from the EU to the US. (see issue 7 of the Belgian Privacy Flash). Since then, companies such as Facebook have been relying on Standard Contractual Clauses or Model clauses for data transfers across the Atlantic.

However, in the Facebook case before the Irish court, Mr Schrems claimed that his data is still subject to violations of fundamental rights when it is being transferred to the US, even if this occurs through the use of so-called "model-clauses". Mr Schrems says that Facebook US is still subject to US mass surveillance laws, and thus he sees *"no way that the ECJ can say that model clauses are valid if they killed Safe Harbour"*.

Consequently, the Data Protection Commissioner intends to challenge the model clauses as a legal basis for international data transfers by referring the Facebook case back to the ECJ.

Belgian Court of Appeal lifts restrictions on Facebook's data collection

On 29 June 2016, the Belgian Court of Appeal annulled the ruling against Facebook ordering it to stop processing personal data of non-users, i.e. users who do not have an account with the social network (see Privacy Flash issue 1).

The Court of Appeal ruled that the Belgian courts do not have jurisdiction over Facebook Ireland, where the data of European users are being processed, nor over Facebook Inc., the US parent company. The Court also stated that there was no urgency to rule on the case since the practice of Facebook has been existing continuously since 2012 and the Belgian court only initiated proceedings for interim relief mid-2015.

Consequently, the social network can continue to collect information in Belgium about internet users who are not registered with the social network site. The Privacy Commission is now focusing on proceedings on the merits, which will be dealt with in September 2017.

Mauritius joins Convention 108

The Convention for the protection of individuals with regards to Automatic Processing of Personal Data, also known as "Convention 108", is the only existing international treaty that grants individuals the right to protection of their personal data. Mauritius acceded to the treaty on 17 June 2018, which brings the total of parties ratifying the treaty to 49 states.

The next countries which will most likely become part of Convention 108 and that have already been invited to accede are Morocco, Senegal and Tunisia.

Recent breaches and enforcement actions

- A mobile advertising company based in Singapore was charged by the Federal Trade Commission because it tracked the location of its consumers without their knowledge or consent, in order to provide them geo-targeted advertising. The company concerned will have to pay $950,000 in civil penalties and implement a comprehensive privacy program to settle the charges. In addition, the company is required to delete all information collected from children.

- The Federal Trade Commission charged an Electronic Health Records company for misleading its consumers. The company solicited patient's reviews of their doctors and posted these on a publicly available website, while patients were led to believe that the information would only be shared with their health care provider. Many of these reviews included patients' full name, phone number or personal health information.

Privacy events around the globe

Right to be forgotten versus right to remember
10 October 2016

Conference organised by the Belgian Data Protection Authority. More information to follow soon.

15th Annual Data Protection Compliance Conference
London, United Kingdom, 13 – 14 October 2016
http://www.pdpconferences.com/find-a-conference/82-15th-annual-data-protection-compliance-conference

This conference organised by PDP aims at providing data privacy professionals with the core tools and necessary information they need to be applied in their daily practice.

International Conference of Data Protection & Privacy Commissioners
Marrakesh, Morocco, 17 – 21 October 2016
https://icdppc.org/news-events/forthcoming-conference-updates/

The International Conference of Data Protection and Privacy Commissioners aims at putting privacy on the agenda in the Arab, Muslim and African regions. The conference will be partly closed and partly open to the public. More information will be published in the coming months.

Conference on the General Data Protection Regulation
Leuven, 18 November 2016

Conference organised by the Belgian Data Protection Authority. More information to follow soon.

European Privacy Academy
Dolce La Hulpe, Belgium, November 2016
http://www.europeanprivacyacademy.com/

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

The next sessions of the European Privacy Academy's DPO Course will take place on:

- 14 – 17 Nov 2016 with follow-up session on 6 Feb 2017
- 08 – 11 May 2017 with follow-up session on 18 Sep 2017
- 13 – 16 Nov 2017 with follow-up session on 5 Feb 2018
- 07 – 10 May 2018 with follow-up session on 17 Sep 2018

Contact us

For further information or an individual consultation on how our Cyber Risk Services experts can help you, please do not hesitate to contact us.

Mark Carter

Managing Partner
Risk Advisory

Dr. Klaus Julisch

Director
Cyber Risk Services