Deloitte.

Switzerland | Cyber Risk Services | Issue 2, February 2016

Privacy Flash
Privacy at your fingertips

Privacy today

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 regular 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, to suggest improvements to the Privacy Flash or to subscribe/unsubscribe, please email us at deloitte.ch.news@deloitte.ch.

Issue 2, February 2016

EU-US Privacy Shield

EU and US reach an agreement on new transatlantic data transfer framework

On 2 February 2016, the European Commission announced a **political agreement** with the US Department of Commerce on a new transatlantic data transfer arrangement to replace the invalidated Safe Harbour framework. The new framework, called "**EU-US Privacy Shield**", will provide EU citizens with several options to exercise their right of redress in the US, including with regards to the use of their data by US national intelligence authorities. The US has also reportedly given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to "clear limitations, safeguards and oversight mechanisms". To ensure that this arrangement does not remain a one-off, an annual review process will be established as well.

Core points of the agreement

- Strong obligations on companies handling EU citizens' personal data and robust enforcement and monitoring by the US Department of Commerce and the US Federal Trade Commission.
- Clear safeguards and transparency obligations on US government access to personal data and assurance in terms of respecting the principles of necessity and proportionality.
- Effective protection of EU citizens' rights with several redress possibilities in front of the Department of Commerce, Federal Trade Commission, an independent Ombudsperson and the set-up of an alternative dispute resolution mechanism that is free of charge. Furthermore companies will be given deadlines to respond to complaints.

Enforcement by regulators

The EU's Data Protection Authorities issued a statement on 3 February 2016 to stress that further analysis of the new Privacy Shield deal is needed to assess whether the arrangement sufficiently addresses the issues raised by the Court of Justice of the EU in the Schrems case. The Article 29 Working Party hopes to receive the official documents related to the EU-US Privacy Shield by the end of February, and is scheduled to **analyse the deal in the first weeks of March 2016**.

While alternative transfer mechanisms such as **Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs) remain valid options** for personal data transfers to the US, the regulators announced that they are assessing "the robustness" of these mechanisms as well in light of the Schrems ruling. By April 2016, the Working Party will provide clarity on the validity of all three options: BCRs, SCCs and the new EU-US Privacy Shield.

In the meantime, the regulators stressed that **relying on the invalidated Safe Harbour framework is in any case illegal** and that regulators will deal with cases and handle complaints on a case-by-case basis. See below for the actions taken by the CNIL against Facebook.

Next steps

The College of Commissioners, the top decision body within the European Commission, has already approved the political agreement reached and has mandated Justice Commissioner Jourová to draft a new "**adequacy decision**". This decision would imply that based on the EU-US Privacy Shield, personal data can be transferred from the EU to the US without further legal safeguards needed. The Commissioner estimated that the arrangement could be implemented and enter into force within 3 months.

However, since the Schrems ruling clarified that it is ultimately up to national Data Protection Authorities to decide whether a personal data transfer complies with the requirements of the EU Data Protection Directive, the success of the EU-US Privacy Shield will hinge on the opinion of the Data Protection Authorities (DPAs) in the Art. 29 Working Party. As explained above, **more clarity is expected by April 2016**.

For further information please see:

- The European Commission press release of 2 February 2016
- The Art. 29 Working Party press release of 3 February 2016
- Fact sheet of the US Department of Commerce of 2 February 2016

US Congress passes Judicial Redress Act

On 10 February 2016, the US House of Representatives approved the Judicial Redress Act again after amendments were made to it by the US Senate's Judiciary Committee in January. The Act was amended by the Senate to include a condition stating that a third country's inclusion would depend on (1) whether it allows companies to transfer personal data to the US for commercial purposes and (2) whether the country has personal data transfer policies that do not materially impede the national security interests of the US.

The Judicial Redress Act would partially extend redress rights enjoyed by US citizens under the Privacy Act of 1974 to citizens of selected covered countries (including EU Member States) and is a precondition for the formal adoption of the EU-US Umbrella Agreement. EU Justice Commissioner Vera Jourová welcomed the Congress' approval of the Judicial Redress Act on Twitter, calling it "another key step to restore trust in transatlantic data flows".

The Act will now be presented to the President to be signed into law.

European member states anticipate privacy changes

As communicated in our previous Privacy Flash, the European Institutions have reached an agreement on a final text for the new General Data Protection Regulation (GDPR). The agreement marks the end of 3½ years of negotiations and lauds the beginning of a new data protection regime in Europe. The Regulation will replace the former 1995 EU Data Protection Directive and create a unified data protection law that will apply directly across all 28 EU Member States as from 2018.

Even though organisations and regulators have a two-year period to prepare for the Regulation, a number of Member States have already anticipated the privacy changes that will enter into force as from Q2 2018.

Romania reduces notification duty

On 28 December 2015, decision 200/2015 came into force in Romania setting out which data processing activities no longer require a notification to the DPA. The Romanian government is thereby anticipating the General Data Protection Regulation which will abolish the notification requirement, replacing it with increased accountability requirements for controllers and processors. However, given the need to ensure effective protection of the rights of the individuals whose data are processed (especially when certain data processing operations present risks to the rights and freedoms of individuals) notification is still necessary in a limited number of cases (e.g. processing of genetic and biometric data). In addition, the processing of personal data for surveillance monitoring (CCTV), as well the transfer of personal data to states not ensuring an adequate level of protection, still need to be notified to the DPA.

New guidance on data breach notification requirements in the Netherlands

In the Netherlands, a new law entered into force on 1 January 2016. The new law empowers the Dutch DPA (now named Autoriteit Persoonsgegevens) to anticipate the requirements of the new General Data Protection Regulation – in the areas of data breach notification and enforcement. More precisely, data controllers are to notify the Dutch DPA immediately of any data security breach that has, or is likely to have, serious adverse consequences to rights and freedoms of data subjects. Furthermore, data controllers have to notify any affected individuals if it is feasible that the breach could have adverse consequences to those individuals, unless the compromised data is encrypted or otherwise made unintelligible to third parties. The DPA has adopted practical guidelines (in Dutch) on 9 December 2015 laying down rules to help organisations identify cases where data security breaches must be reported to the DPA and individuals.

In terms of enforcement, the new Dutch law also empowers the DPA to impose fines up to €820,000 for violations of the Dutch data protection law, such as failure to report data security breaches. The level of fines, violations and categories of sanctions are defined in draft guidance, published in October 2015.

European Court of Human Rights rules on employee monitoring

Recently, the European Court of Human Rights released a judgement in Bărbulescu v. Romania on the possibility for employers to monitor their employee's internet use in certain circumstances.

In summary, Bărbulescu was dismissed by his employer, a private company, for having used the company's internet for personal purposes during working hours, this being in breach with internal regulations. In front of the Court, relying on Article 8 of the European Convention of Human Rights (the "ECHR", right to respect for private and family life, the home and correspondence) Bărbulescu complained that his employer's decision to terminate his contract followed a breach of his privacy.

The Court considered that the fact that the employer had accessed Bărbulescu's professional internet account and that the record of his communications had been used in the domestic court case to prove the employer's case was sufficient to engage the applicant's "private life" and "correspondence". It therefore found that Article 8 ECHR was applicable. However the Court ruled it was "not unreasonable for an employer to want to verify that the employees are completing their professional tasks during working hours" and "noted that the employer had accessed Bărbulescu's account in the belief that it contained client-related communications". The Court took into account that the employee had created a Yahoo Messenger account upon request of his employer and that, according to the employer's regulations, this account could only be used for the purpose of responding to clients' enquiries. Furthermore the Court stated the monitoring was proportional and in accordance with the scope of the internal regulations of the company, as the employer had only accessed the employee's Yahoo Messenger account and did not monitor any other documents stored on his computer.

The Court therefore decided that there was no violation of Article 8 of the ECHR in this case as the Romanian courts had struck a fair balance between Bărbulescu's right to respect for his private life and correspondence and the interests of his employer.

Read the press release of the Court's decision here.

European Parliament votes on NIS Directive

On 14 January 2016, the European Parliament's internal market committee voted on the Network Information Security Directive (NIS). As mentioned in the previous issue of the Privacy Flash, the European Parliament and Council reached an informal agreement on 7 December

2015 on the proposed Network Information Security Directive (NIS), which aims at increasing cooperation between Member States and lay down security obligations for operators of digital service providers (online marketplaces, search engines and cloud computing services) and so-called “essential services”. This scope puts public and private entities in the financial services, energy, transport, health, water and digital infrastructure sectors with more than 50 employees within the remit of the law as well.

The NIS Directive will introduce a security incident notification requirement that extends beyond the personal data breach notification requirements of the GDPR. While the GDPR obliges organisations to report a breach only when the risk to the privacy of data subjects is high, the NIS Directive requires operators to notify the authorities whenever a security incident (any event having an actual adverse effect on the security of networks and information systems) has a substantial impact on the provision of their services.

Before the new rules can enter into force, the Directive will still have to be formally adopted by both law-making institutions of the EU, the Parliament and the Council. This is expected to happen in Spring 2016, according to the European Council’s press release. After the formal adoption of the Directive, the Member States will have 21 months to transpose its provisions into national law.

More detailed information on this topic is available on the Belgian Deloitte website.

Facebook appeals Belgian court order to stop tracking non-account holders; the CNIL follows Belgian DPA

As mentioned in our previous Privacy Flash, on 9 November 2015, a Belgian court ordered Facebook to stop processing personal data of Belgian internet users who do not have a Facebook account. The court case was launched by the Belgian DPA, the Privacy Commission, in response to the findings of a study that it had commissioned, showing that Facebook tracked internet users without a Facebook account through so-called “datr”-cookies. The court ordered Facebook to stop this practice before 14 December 2015, placing a penalty of €250,000 per day for non-compliance after that date.

On 28 January 2016, Facebook appealed to the Belgian Court of First Instance arguing that the entire ruling must be nullified. On 8 February 2016, the CNIL, the French DPA also publicly issued formal notice to Facebook to comply with the French Data Protection Act within three months, for the same reasons as the Belgian court and due to Facebook’s data transfers under Safe Harbour (note: the Schrems judgement of October 6, 2015 was made in a case against the Irish DPA relating to Facebook).

Considering the investigation on Facebook's cookies was done in cooperation between the Belgian, Dutch, French, German (Hamburg) and Spanish DPAs, we will keep track of the actions the Dutch, Hamburg and Spanish DPAs (and others) will take.

European Watchdog publishes working programme for 2016

The European Data Protection Supervisor (EDPS) has announced its main priorities for the New Year on 7 January 2016. Through its working programme, the EDPS lists key actions that will maximise the impact of its work on privacy and data protection at EU level.

The EDPS is an independent supervisory authority responsible for monitoring data processing by EU institutions, advising on privacy policies and legislations and cooperating with similar authorities to ensure a consistent level of data privacy.

The EDPS is planning to advise on a number of legal instruments which include: the completion of the new EU data protection framework (Regulation and Directive) that was adopted in December 2015, advising on the review of Regulation 45/2001 that lays down data protection rules for EU institutions and bodies and contributing to the work in reviewing the e-Privacy Directive.

Furthermore the EDPS not only prioritises the need, it will also comment on legal frameworks for transatlantic data transfers such as the EU Commissions Implementing Decision on EU-US data flows (adopted following the Schrems ruling tearing down the Safe Harbour framework) and will follow the EU Commission's work to make sure that data privacy is taken into account in international agreements (e.g. EU-US Transatlantic Trade and Investment Partnership). Other priorities include advice to, and cooperation with, the EU co-legislators with a view to elaborating balanced and efficient legislative and policy proposals in areas such as security and combatting of terrorism or the implementation of the EU Digital Single Market Strategy.

Russia's "right to be forgotten" law enters into force

On 1 January 2016, the Russian "right to be forgotten" law, signed by President Putin on 13 July 2015, entered into force. This law amends the Russian Federal Law "On Information, information technologies and on protection of information" (No. 149-FZ of 27 July 2006). It obliges search engines that publish advertisements directed towards private individuals located

in Russia, to remove search results listing information on individuals that is unlawfully circulated, untrustworthy, outdated or irrelevant.

Search engines are to be understood as information systems that undertake web searches and publish information hosted on third parties' websites, i.e. search engines such as Google. The new Russian law does not clarify the criteria which define whether an advertisement is directed towards Russian consumers. However it is assumed that the following criteria will likely be based on: websites employing Russian top level domains e.g. .SU, .RU, .RF; websites and advertisements written in Russian (even when not using a Russian top level domain).

The lower chamber of the Russian Parliament (i.e. State Duma) is planning to introduce a bill establishing heavy administrative fines up to EUR 34.000 for non-compliance with the principles on the right to be forgotten. The Bill still needs to pass two more readings in the lower chamber, is to be approved by the upper chamber (i.e. Federation Council) and to be signed by President Putin before it becomes official law.

Taiwan amends Personal Data Protection Law

At the end of December 2015, Taiwan's Office of the President took a decision to amend 12 provisions of Taiwan's Personal Data Protection Law. The revision enhances the collection and use of sensitive personal data, the format of consent for the collection and use of non-sensitive personal data, and the burden of criminal liability for violations of some requirements of the Personal Data Protection Law. The amended provisions will enter into force in the first half of 2016.

On the matter of non-sensitive data, the revision entails the deletion of the requirement that government entities or private sector entities are to obtain written consent of the data subject in order to collect, process or use non-sensitive data. In addition, the revision demands written consent for "special" categories of personal data (i.e. sensitive personal data incl. medical records, information on medical treatment, genetic information, sexual background, criminal records and health examination information. Furthermore, proper security measures need to be put in place prior or after the collection processing or use of special personal data.

Penalties for infringement of the Personal Data Protection Law will be fixed to an imprisonment of up to 5 years and a maximum fine of approximately $30,000. These fines are only to be applied when an infringement was intended to safeguard illegal interests for oneself or a third party, or to infringe upon the interests of others.

Recent breaches and enforcement actions

- The US regulator in charge of privacy, the Federal Trade Commission (FTC), has agreed to settle with a dental practice software provider for $250,000 over charges that accused the company of falsely advertising the level of encryption it used to protect patient data.
- The UK Information Commissioner Officer (ICO) has demanded for stronger enforcement powers to deter data thieves. The call for heavier sanctions came after the occurrence of a woman selling 28,000 pieces of sensitive driver data who was fined only £1,000.

Privacy events around the globe

Global Privacy Summit 2016

Washington DC, USA, 5-6 April 2016
https://iapp.org/conference/global-privacy-summit-2016

The Global Privacy Summit is the largest and most-anticipated privacy event in the world. It brings together a wide range of privacy professionals to advance the privacy conservation, address privacy challenges of our time and provide a unique networking opportunity

6th European Data Protection Days 2016

Berlin, Germany, 25-26 April 2016
http://www.euroforum.de/edpd/

The event will discuss the latest developments in data protection with the data privacy institutions, privacy officers and data protection specialists from all over the world. Main topics that will be addressed are the EU General Data Protection Regulation, the EU-US Privacy Shield and other privacy developments around the world.

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
markjcarter@deloitte.ch

Dr. Klaus Julisch
Director, Cyber Risk Services
kjulisch@deloitte.ch

Deloitte AG
General-Guisan-Quai 38
8022 Zurich
Switzerland