Deloitte.



# 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 of our regular news flash 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 5, June 2016 Highlights**

## General Data Protection Regulation

### GDPR publication in the Official Journal of the EU

On 4 May 2015, the General Data Protection Regulation was published in the Official Journal of the European Union. The new European data protection regime will apply as from 25 May 2018: 2 years and 20 days following the publication in the European Official Journal. The Regulation will replace the former 1995 EU Data Protection Directive and create a unified data protection law that will apply directly in all 28 EU Member States.

Starting 25 May 2020, the European Commission will present a report on the GDPR to the European Parliament every four years. These reports will include an evaluation and review of the Regulation and will be available to the public. European businesses are thus expected to be GDPR compliant within two years. They should start their preparation process right now.

### France anticipates GDPR changes

France is anticipating the upcoming GDPR changes through its draft bill for a Digital Republic. The draft bill was adopted by the French National Assembly in first reading on 26 January and amended by the Senate on 3 May 2016. The new bill introduces a series of obligations and GDPR-inspired provisions. It would give the CNIL the same power to issue fines as will be the case under GDPR as from May 2018, it introduces a right to data portability, class action lawsuits and stipulates the obligation for controllers to inform data subjects about envisaged retention periods.

The Senate proposes a new data-localisation provision, which demands that personal data is stored in data centres localised in the European Union and prohibits the transfer of data to a non-EU third country. The rationale behind this is to ensure that European standards apply to French data, especially against the background of the Safe Harbour ruling of the European Court of Justice.

It is under discussion whether the new provision can be justified against the background of the GDPR. According to article 23 of the GDPR, countries have a margin to restrict the scope of rights and obligations at local level, however this article does not apply as such to international data transfers. Due to these inconsistencies, it is reportedly unlikely that the draft bill will be adopted.

### UK Data Protection Authority anticipates GDPR changes

On 24 May 2016, the UK Data Protection Authority (ICO) set out what businesses can expect to receive in terms of guidance on how to prepare for the GDPR. The ICO's guidance will be created in three phases:

**In phase 1,** the ICO will help organisations understand the difference between the GDPR and the old EU Directive, as well as focus on the key provisions of the Regulation. It will publish its own guidance regarding individuals' rights, contracts, consent and privacy notices in the next six months. In addition, it will contribute to the Article 29 Working Party's programme for 2016, which will deliver advice on the following topics by the end of the year:

- Identifying an organisation's main establishment and lead supervisory authority
- Data portability
- Data Protection Officers
- Risky processing and Data Protection Impact Assessments
- Certification

**In phase 2**, a more detailed guidance structure will be created, including a plan that will show organisations and the public the guidance to be available before and after May 2018. In addition, the ICO will create practical tools and resources to assist organisations, especially small and medium sized enterprises (SMEs) in improving their compliance.

**In phase 3,** the actual guidance will be written and published and the aforementioned tools will be developed. This guidance will then be regularly reviewed and updated based on the experience developed by the ICO "through queries, approvals, enforcement and court judgments as well as feedback about practical issues and implications from stakeholders".

## NIS Directive adopted by the EU Council

On 17 May 2016, the EU Council formally adopted the Network and Information Security (NIS) Directive. After the EU Council has transmitted its vote, the European Parliament will submit a vote in July 2016. The NIS directive is expected to formally enter into force as from August 2016.

As stated in Issue 1 of the Privacy Flash, the NIS Directive aims to increase cooperation between Member States. It lays down security obligations for operators of digital service providers (online marketplaces, search engines and cloud computing services) and so-called "essential services". The scope of the Directive 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.

From a privacy perspective 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 for the privacy of the 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.

# International Data Transfer mechanisms in limbo

## Privacy Shield faces difficulties

Discussions are continuing at a European level on the matter of international data transfers to the U.S. and the newly proposed Privacy Shield. The Shield has been negotiated between the European Commission and the US Department of Commerce and was designed to replace the former Safe Harbour framework after its invalidation in the Schrems case. The European Commission has drafted an adequacy decision, which once adopted will ensure that equivalent safeguards to data protection standards in the EU are in place when transferring data to the US under the new EU-US Privacy Shield.

The EU-US Privacy Shield will enforce strong obligations on companies and insert a "robust supervision mechanism" as it will (1) insert strong limitations and safeguards to US government officials to access personal data for law enforcement and national security purposes, (2) ensure that the EU citizen's rights are protected effectively with the possibility for redress and (3) introduce an annual joint review mechanism to assess the functionality of the EU-US Privacy Shield.

As outlined in a previous issue of the Privacy Flash, the Article 29 Working Party released its non-binding Opinion on the Privacy Shield following the publication of the draft adequacy decision by the European Commission on 29 February 2016. In the meantime the Article 31 Committee, composed of representatives of all member states and chaired by a European Commission official, was supposed to reach an agreement on the Privacy Shield on 19 May 2016. The Committee, which has veto power and can thus block the adoption of the adequacy decision, failed to reach a consensus.

Furthermore, on 26 May 2016, the European Parliament issued a resolution stating that the European Commission should proceed in negotiating with its U.S. counterparts to counter the deficiencies in the proposed Privacy Shield, in particular concerning:

- The possibility for US authorities to access data transferred for commercial purposes;
- The remaining possibility to conduct bulk collection of personal data in non-compliance with the EU principles of necessity and proportionality and the EU Charter of Fundamental Rights;
- The independence and authority of the Ombudsman;
- The redress mechanism, which is deemed to be too complex to be understood by the data subject and lacks user-friendliness.

Finally, the European Data Protection Supervisor (EDPS) also issued an opinion on the Privacy Shield, arguing that a more robust and sustainable solution is needed. "Significant improvements are needed should the European Commission wish to adopt an adequacy decision, to respect the essence of key data protection principles with particular regard to

necessity, proportionality and redress mechanisms", said Giovanni Butarelli of EDPS.

## EU model contracts to be challenged before the Irish Courts

The Irish Data protection authority has expressed its intention to launch legal proceedings to the Court of Justice of the European Union to challenge the validity of EU model contracts. This unofficial statement of the Irish DPA follows the previous decision of the Court of Justice of the European Union declaring the Safe Harbour framework invalid on 6 October 2015 in the so-called Schrems case for not being adequate according to the European standards.

Max Schrems stated on 24 May 2016 that Facebook U.S. proceeds to be subject to mass surveillance activities, irrespective of the use of EU model contracts instead of the invalidated Safe Harbour framework. Schrems argues that data transferred to the U.S. remains subject to fundamental rights violations and that EU model contracts consequently should not be considered a valid mechanism for international data transfers to the US either.

## French Data Protection Authority issues 2016 inspections programme topics

The French Data Protection Authority (CNIL) has published its main priorities for 2016. The CNIL is planning to carry out a number of online, on-site and record inspections concerning the following topics:

- Health databases
- Flight passengers' data
- Data for marketing

The CNIL will furthermore work together with other European Data Protection Authorities during a Sweep Day focusing on health and well-being devices and privacy of home devices. This initiative will examine the quality of the information notices to customers, the security of data flows and the degree of customers' control over the use of their personal data. The outcome of the Sweep will be published later this year.

## Supreme Court ruling in Spokeo v. Robins

On 16 May 2016, the U.S. Supreme Court ruled in the Spokeo Inc. v. Robins case. Spokeo Inc., a company operating a "people search engine on the Internet", collects publicly available personal data from various sources and uses it to create personal profiles that its users can retrieve. The plaintiff Thomas Robins alleged that inaccurate information in his profile may have negatively impacted his chances of finding a job. Based on the 1970 Fair Credit Reporting Act (FCRA), which requires consumer reporting agencies to "follow reasonable procedures to assure maximum possible accuracy" of consumer reports, he sued Spokeo.

The Court ruled in favour of Spokeo, leading to what US privacy advocates consider a "potential set-back for the privacy rights of all users". The Court explained that a violation of Robins' statutory rights under the Fair Credit Reporting Act (FCRA) in itself does not provide standing and that Robins should have demonstrated that he suffered "injury in-fact" due to Spokeo's publication of incorrect information about him.

The case has now been sent back to the Ninth Circuit Court, which will re-evaluate Robins' claim under a more specific test.

## "IP addresses are personal data"

On 12 May 2016, an opinion was released by Advocate General Sanchez-Bordona of the European Court of Justice stating that IP addresses are personal data. The opinion was released in relation to a court case whereby a German privacy activist, Patrick Breyer, sued the German government over logging all visits to government websites.

Breyer urges the European Commission to amend the European legislation to prohibit any blanket recording of individuals' internet use by website operators. The Advocate General did not state whether website operators may or may not retain IP addresses in bulk but did acknowledge however that IP addresses are data that either by themselves or in combination with other data, can be considered personal data.

## Belgian court rules on right to be forgotten

In a judgment issued on 12 May 2016, the Belgian Court of Cassation, the country's highest court, decided that the right to be forgotten applies to electronic archives of newspapers as well. The newspaper Le Soir lost the case against an individual who had been convicted in a traffic accident case.

The Court argued that the online publication of a case from over twenty years ago (the accident was reported on in Le Soir in 1994), was likely to cause damages to the individual in the present. This would affect the individual's right to privacy to an extent that the Court regarded as disproportionate in relation to the interests of the newspaper in its right to freedom of expression. The defendant group Rossel, which owns the newspaper, called the judgement one that "opens the door for a rewriting of history".

## New data retention law in Belgium

On 4 May 2016, a new draft data retention law governing the telecommunications sector was approved by the Belgian Parliament. As reported in a previous issue of the Belgian Privacy Flash, the Constitutional Court of Belgium had invalidated the old data retention law, which mandated a two-year retention period for all meta-data related to telecommunications traffic.

The new law lays down a one-year retention period and includes rules on the access of the data by enforcement and public authorities. The extent of access is made conditional on the severity of the crime or violation that necessitates the request for access to the phone records. For minor offences, no access is granted; for other crimes, access can be granted up to six months. Only in the context of the most severe crimes can law enforcement consult the full year of retained phone records.

## New Secretary of State for privacy appointed in Belgium

On 2 May 2016, a new state secretary for privacy was appointed in Belgium. Now former Member of European Parliament Philippe De Backer replaces Bart Tommelein, who has taken up a minister post in the Flemish Government. De Backer announced that he is planning to reform the Belgian Data Protection Authority (Privacycommissie) in anticipation of the improved powers that DPAs will have under the EU General Data Protection Regulation. In the coming months, the State Secretary will consult with the Belgian Parliament, the Privacy Commission, as well as with consumers and stakeholders in order to define a reform strategy.

## Recent breaches and enforcement actions

- The UK Information Commissioner Officer (ICO) has fined a claims management company £250,000 for conducting nuisance calls. Companies making calls that play a recorded message can only do so if they have gained specific permission from individuals to make that type of call and if they identify themselves within the message.

- The UK Information Commissioner Officer (ICO) has fined an EU campaign office £50,000 for sending text messages to people without their consent to support their campaign to leave the European Union.

- Social network LinkedIn issued a data breach notification to affected users after the e-mail address and passwords of over 100 million accounts were put up for sale online. The breach is related to a data theft which took place in 2012, leading LinkedIn to invalidate the passwords of all accounts which had not changed passwords in over four years.

## Privacy events around the globe

### Privacy Laws & Business 29th Annual International Conference

St John's College, Cambridge, United Kingdom, 4 - 6 July 2016
http://www.privacylaws.com/annual_conference/

The conference will address a wide range of topics such as the EU General Data Protection Regulation, the Cloud and the Internet of Things, Mobile apps and wearables, Connected health, the concept of consent, and more.

## 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

The 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.

## 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 trainings.

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