Deloitte.

Switzerland | Cyber Risk Services | Issue 3, March 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 3, March 2016

News on General Data Protection Regulation

Formal adoption by Council and EP

The European Institutions announced on 15 December 2015 that they reached a political agreement on the final text for the new General Data Protection Regulation (GDPR). Upon approval by the responsible LIBE Committee of the European Parliament on 17 December 2015, the agreement was also approved without any debate on 12 February 2016, during an Economic and Financial Affairs meeting of the EU Council.

Consequently, the text will now be submitted for formal adoption by the EU Council, most likely in the Justice and Home Affairs configuration. The next formal meetings of the Justice and Home Affairs Council take place on 10-11 March and 9-10 June 2016. Once the Council has formally adopted the text, it can be sent to the Parliament for a vote in plenary session.

Upon formal adoption by both bodies, the official text of the Regulation will be published in the Official Journal of the EU. Two years after the publication date, the new rules will then officially enter into force.

More information on the General Data Protection Regulation is available on the Deloitte website.

GDPR action plan of Article 29 Working Party

On 11 February 2016, the Article 29 Working Party (WP29) adopted a statement on its 2016 action plan for the implementation of the General Data Protection Regulation (GDPR). The action plan defines four priorities for this year in order to prepare the entering into force of the GDPR in 2018. The first priority is the set-up of the European Data Protection Board's (EDPB) structure in terms of administration, such as IT, human resources, budget and service level agreements. Secondly, the-one-stop-shop and the consistency mechanism will be developed. In order to help controllers and processors prepare for the GDPR, a third priority of the action plan is to provide guidelines on topics such as the new right of data portability, the data protection officer, certification, notion of high risk and Data Protection Impact Assessment. Lastly, the WP29 recognised the communication around the EDPB/GDPR as a priority, in order to make this new legal body visible as a key player.

The WP29 will review this action plan periodically and will further complement it in 2017 with new objectives and deliverables.

France plans to adopt GDPR elements before 2018

The French Government introduced a "Digital Republic Bill" that would amend several provisions of the GDPR. After the French National Assembly adopted the Bill in January, it was passed to the Senate that is expected to decide on the matter and adopt the Bill, later this year. Some of the key provisions of the French Bill that would be applicable even before the GDPR provisions enter into force, concern the following subjects: the right to data portability, information of the data subject, rights of the data subject, right to erasure (right to be forgotten), sanction powers of the CNIL (the French data protection authority), cooperation of the CNIL with other DPAs, anonymisation procedures, and class actions.

German consumer protection organisations get class action powers for data protection violations

On 17 February 2016, Germany published the "Act to improve the civil enforcement of consumer protection provisions of data protection law". This Act provides consumer protection associations the right to initiate court actions on behalf of individuals. Generally, lack of resources of the authorities and low (to none) financial loss on individuals led to a low level of data protection enforcement in court, especially for violations in the fields of advertising (not respecting opt-outs), selling personal data to third parties, profiling, etc. The GDPR foresees a similar provision.

An interesting fact is that for violations against rules concerning international data transfers (e.g. transfers under Safe Harbour), it will only be possible to make claims starting from 1 October 2016.

The German DPAs will have a role to play in these proceedings as they will be able to express their opinion and analysis of the alleged violations in court.

When a consumer protection association files a privacy case, the court will not be able to award damages, but it will be able to issue cease-and-desist letters and interim injunctions

News on EU-US data transfers

Judicial Redress Act signed by President Obama

On 24 February 2016, President Barack Obama signed the Judicial Redress Act ("the Act") into law, which is a step forward in the EU-US data transfer discussion. As President Obama stated, the Act *"makes sure that everybody's data is protected in the strongest possible way with our privacy laws – not only American citizens, but also foreign citizens".*

The same day, a statement by Commissioner Vera Jourová was published stating that *"the Judicial Redress Act will ensure that all EU citizens have the right to enforce data protection rights in U.S. courts. U.S. citizens already enjoy this right in Europe".* As highlighted in the

previous article, the adoption of the Judicial Redress Act is crucial for the adoption of the EU-US Privacy Shield (see further below) and the EU-US Umbrella Agreement.

European Commission publishes legal texts on the EU-US Privacy Shield

On 29 February 2016, the European Commission published the legal texts that will establish the EU-US Privacy Shield, including a draft adequacy decision, Frequently Asked Questions and a Communication that summarises the actions taken to restore trust in transatlantic data flows since the 2013 Snowden revelations. This event follows the political agreement on the EU-US Privacy Shield that was reached on 2 February 2016 between the European Commission and the US Department of Commerce.

Once adopted, the European Commission's adequacy decision 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 new framework reflects the requirements set by the European Court of Justice in the so-called Schrems ruling from 6 October 2015, declaring the Safe Harbour framework invalid. The European Commission communicated in its press release that the "U.S. authorities provide strong commitments that the Privacy Shield will be strictly enforced and assured there is no indiscriminate or mass surveillance by national security authorities".

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.

The requirements to US organisations for registering on the Privacy Shield will be similar as under Safe Harbour. American companies will need to register and self-certify annually that they meet the requirements set out. First and foremost, they are to comply with the (renewed) Privacy Principles of "Notice", "Choice", "Security", "Data Integrity and Purpose Limitation", "Access", "Accountability for Onward Transfers" and "Recourse, Enforcement and Liability". As under Safe Harbour, companies will have to state publicly that they comply with the Privacy Shield. While it's too early for a detailed comparison between the Privacy Principles under Privacy Shield and Safe Harbour, a first analysis shows that the new Privacy Principles will be more prescriptive than the Safe Harbour Privacy Principles (e.g. on onward transfers), but not to the level of the upcoming EU General Data Protection Regulation. The main shift will be on heavier compliance monitoring by the FTC (which will be monitored by the EU), the additional rights for individuals (e.g. filing a complaint through their local EU DPA and the enhanced dispute resolution requirements) and further restrictions for US intelligence practices.

In its Communication, the European Commission lays down the actions that are to be taken by the different actors (i.e. US companies, US authorities, European Data Protection Authorities and the Commission). Furthermore, companies are urged to prepare to join the new framework as soon as possible.

Next steps

It is now up to the committee composed of representatives of the Member States to be consulted. Next, the Article 29 Working Party which brings together all 28 privacy regulators of the EU Member States, will have to adopt an opinion on the new framework. On 29 February 2016, they stated to publish their non-binding opinion on their next plenary meeting which will take place on 12 and 13 April 2016. Afterwards a final decision of the College of Commissioners will be made. Meanwhile, the US authorities are expected to make all the necessary preparations in order to implement to new adequacy framework.

Facebook battle expands into France

The Facebook battle in France concerns the fair collection of personal data of internet users who do not have a Facebook account. This legal battle is similar to the action in Belgium last year, where the DPA imposed a daily fine of 250,000 EUR on Facebook (the case is currently in appeal). In France, the Data Protection Regulator, the CNIL, issued a formal notice last month to Facebook to comply with the French Data Protection Act within three months.

The CNIL requires changes in 11 topics, including:

- A stop to combining information of users for marketing purposes without legal grounds (consent)
- A request to explicitly consent with processing sensitive personal data (such as religion for instance)
- A compliant processing of data of internet users without a Facebook account collected through the datr cookie and like buttons
- Storage of personal data for a limited period of time (such as deleting IP addresses after 6 months after last access to an account)
- The use stricter password requirements
- Ceasing data transfers under Safe Harbour (and hence implement an alternative mechanism)

Both in France and in Belgium, Facebook has responded that the use of the datr cookie is necessary for security purposes.

Google expands right-to-be-forgotten rule

Privacy regulations in Europe demanded that Google expand its right-to-be-forgotten rule. Until now, Google removed search results only across its EU sites. However, when the rule does not cover all search sites of Google, users would still be able to retrieve delisted URLs simply by using google.com to perform searches.

Google explained on 4 March 2016 that "in addition to the existing practice, they will also use geolocation signals (like IP addresses) to restrict access to the delisted URL on all Google Search domains, including google.com, when accessed from the country of the person requesting the removal. The changes will be applied retrospectively."

In practice, this would mean that a person located in Germany for example would not be shown the link to a URL which was delisted after a German request on any of the Google Search domains. The link would, however, still be shown to a person located in the UK when using a non-European Google Search domain. At this point in time, it is unclear whether the expansion of the rule will satisfy the European privacy regulators. The CNIL stated it will look into it.

Recent breaches and enforcement actions

- An investigation by the Dutch Data Protection Authority (AP) has led a Dutch transport company to cease filming its drivers on a constant basis. The company used these images to discuss and improve the driving behaviour of its employees. However, the Dutch DPA considered the filming as disproportionate, since it implied a constant monitoring of the employees.
- The UK Information Commissioner's Office (ICO) has issued a fine of £70,000 for a UK firm that made thousands of nuisance phone calls between 1am and 6am. In the same week, another firm that was cold calling people registered with the Telephone Preference Service was fined £80,000 by the ICO.
- On 29 February 2016, the ICO issued its largest ever fine of £350,000 for a lead generation firm responsible for over 46 million automated nuisance calls. The regulator had received over 1,000 individual complaints related to the case.
- In spring 2014, the French Data Protection Authority, the CNIL, carried out an inspection on a telecom operator and its subcontractors following a security breach jeopardising the personal data of more than one million customers. In August 2014, the CNIL formally issued a warning to the company for (a) not having performed a security audit on the processor, (b) sending data to the processor in a non-secure way and (c) not having included any security or confidentiality clauses in the contract with the processor. The

telecom operator had disputed the warning in court, which has now led to the French Council of State confirming the CNIL's initial decision.

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.

European Privacy Academy

9-12 May 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.

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
mjcarter@deloitte.ch

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

Deloitte AG
General-Guisan-Quai 38
8022 Zurich
Switzerland