Privacy Flash – Issue 9

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

Highlights

News

Russia blocks LinkedIn after non-compliance with data localisation requirement

As already mentioned in issue 6 of the Belgian Privacy Flash and issue 7 of our newsletter, the Russian DPA Roskomnadzor has taken a very pro-active point of view with regards to the data protection of Russian citizens. It has adopted a localisation requirement which stipulates that all data regarding Russian citizens shall be stored in data centres on Russian territory. It initiated a range of enforcement actions to ensure a strict follow-up of this new rule.

Whereas Google and Facebook have opted to follow the provisions, a recent judgement showed a non-compliance from LinkedIn, refusing to store the data in Russia. This judgement was a confirmation of the decision taken by the District Court of Moscow with regards to the negative inquiries by the Russian DPA into LinkedIn. As a consequence, Russia required all local Internet Service Providers to block access to the site.

In the meantime, the social networking site has responded to the events and has sent a letter to the Russian DPA to request a meeting. It remains to be seen whether the meeting shall take place and will have a more positive outcome for LinkedIn and its Russian users.

UK Investigatory Powers Bill enters into force

On 29 November 2016, the Investigatory Powers Act has officially been given royal assent, meaning that the implementation will be due very soon. Since its introduction last year, the act has been widely criticised by various stakeholders and privacy activists and has been mockingly referred to as the 'snoopers charter' because of the extended powers of the UK government in the area of surveillance.

An illustrative example is that companies will be obliged to support the government in bypassing encryption unless it is not achievable in practice.

While the act intends to take great leaps, the UK government prefers a careful approach and have some of the investigatory powers tested before using them in practice. While the adoption already did not go off without a hitch, the implementation might run into even more difficulties. A petition has been started requesting the repeal of the Act. An overwhelming amount of signatures has already been received and it is said to possibly be one of the most popular petitions ever. Whether the petition will have an actual influence on the implementation of the Act, is not clear at this point.

Class actions for data protection become possible in France

On 19 November 2016, the French government published a new act called 'the modernisation of justice' which includes provisions on class actions taking place within the French territory. Where the previous act of 2014 only had a limited scope, the newly adopted act covers a great range of topics, including data protection.

The act is based on the idea that a specifically enlisted set of organisations has the right to take collective action against any violation of the French data protection legislation and may defend the rights of all individuals that could be or are being harmed by the situation.

France is not the first country to allow such data protection actions, Germany has also provisioned class actions in its national laws. It must be pointed out however that France seems to have taken a more restrictive approach than the other countries, as it is limiting the use of class actions only to cases where it is needed to help cease the breach. These actions will not lead to any compensation.

Argentina introduces its proper set of Standard Contractual Clauses

The Argentinian DPA has recently published a Regulation on international data transfers, which introduces a set of Standard Contractual Clauses, similar to the ones used by the EU in its data transfer cooperation.

The Standard Contractual Clauses were established as a response to a generally existing need to update the Argentinian law to worldwide business standards. As is the case in the EU, the Argentinian DPA has identified those countries that ensure an adequate level of data protection and to which personal data can be sent without additional safeguards.

By means of these contracts, the Argentinian DPA now allows cross-border transfers to all countries, as long as the contracts are used and are notified to the Argentinian DPA.

German draft GDPR implementation law published; Angela Merkel's call for a more 'business-friendly' German data protection law

The German government has recently published a new draft for the implementation of the impending GDPR. While it seems that the amount of obligations for data controllers is indeed decreasing, some also state that the act might impact the rights of the individuals. It will be interesting to see what the stance of Germany is when the final version of the act has been published.

In this respect, it is interesting to note that during a speech recently held at the 10th National IT Summit, German Chancellor Angela Merkel shared her wish for a more enterprise-friendly German data protection law. In general, Germany is known for its very proactive stance in all data protection matters and the statement was therefore applauded by several entities, including data protection Minister Dara Murphy from Ireland.

During this speech, Mrs Merkel expressed her concerns that Germany might miss out on important digital evolutions if it does not change it standards to a more business-minded approach. In this respect, she pointed out the topic of data minimisation that may have been interpreted too restrictively in Germany, as it does not really allow to fully engage in big data analytics.

European Parliament green light for the EU-US data protection Umbrella Agreement

It has been a long timing coming but after the European Commission has signed the EU-US Data Protection 'Umbrella Agreement' on 2 June 2016, the European Parliament has now approved the agreement as well.

In a resolution dated 26 March 2009, the European Parliament expressed the need for a transatlantic agreement to ensure adequate protection of civil liberties, including the right to data protection when sharing data in the context of fighting crime and terrorism.

The negotiations about this agreement were difficult, especially because of cultural differences between the EU and US in the field of data protection and the Snowden revelations in 2013 about mass spying by the NSA and thus exposing the risk of mass surveillance by the US.

The agreement itself is not a legal instrument that allows the transfer of personal data to the US; it contains data protection safeguards which should be implemented when transferring personal data following existing or future data transfer agreements.

The greatest asset of the new 'Umbrella Agreement', is the judicial redress. This entails that EU citizens will have the same rights as US citizens when they seek judicial redress before courts in the US in case the US authorities deny access or rectification or unlawfully disclose their personal data.

The only thing left to be done is for the different parties to adopt internal procedures so that it can enter into force. For the EU, this means an adoption of a decision by the Council on the agreement, while for the US, the necessary designations under the Judicial Redress Act shall have to be made.

Facebook temporarily paused using users' data from WhatsApp

As mentioned in issue 7, WhatsApp announced in August 2016 that it would update its Terms and Conditions to allow user information to be shared with Facebook. In the meantime, Facebook confirmed earlier this month that it will temporarily pause the use of European WhatsApp user data for advertising and product-improvement purposes.

In August, Head of the Information Commissioner's Office (ICO) Elizabeth Denham, expressed her concerns about consumers not being properly informed about what Facebook plans to do with the users' data collected and that no valid consent has been obtained. "We think consumers deserve a greater level of information and protection, but so far Facebook hasn't agreed", Denham said.

In September, German data protection authorities also expressed concerns and prevented Facebook from collecting data from WhatsApp. Johannes Caspar, Hamburg's Commissioner for Data Protection and Freedom of Information argued that Facebook is required to obtain its users' consent in advance.

In an open letter dated October 2016, the Article 29 Working Party criticised WhatsApp for sharing its users' data with Facebook and requested the app's chief executive to suspend these activities until legal safeguards are in place.

Upon pressure by the ICO and the Hamburg DPA Facebook agreed to pause using the users' data for advertisement and product-improvement purposes. This decision allows both parties to formulate their concerns and discuss the necessary safeguards.

ICO has confirmed that they will keep pressuring this issue, hopefully together with the DPA from Ireland, considering Facebook's European headquarters are located in Ireland.

CNIL shares results of GDPR public consultation

In June 2016, CNIL launched a public consultation about the GDPR *(General Data Protection Regulation)* to professionals, in order to gather concrete questions, difficulties of interpretation and examples of good practice.

The CNIL consultation consisted of 4 different areas of focus:

- The DPO: The definition of the role of the Data Protection Officer in organisations.
- Data portability: The GDPR strengthens the rights that individuals have to control their own data and gives individuals the right to request a transfer of their personal data from one controller to another.
- DPIAs: The GDPR introduces Data Protection Impact Assessments (DPIA) as a means to identify high risks to the privacy rights of individuals when processing their personal data.
- Certification and labelling: about the introduction of data protection certification mechanisms and data protection seals and marks.

The consultation closed on17 July 2016. 540 contributions were submitted and almost 1000 votes issued. It ties in perfectly with the FabLab intiative of the Article 29 Working Party, as pointed out in issue 8, in which the Article 29 Working Party also obtained stakeholder input on the four GDPR aspects listed above.

UK to implement GDPR regardless of Brexit. ICO highlights future guidance of the Article 29 WP on the GDPR

Last month, during her appearance before the Culture, Media and Sports Select Committee, UK Secretary of State Karen Bradley announced that the UK shall implement the GDPR in May 2018 regardless of the circumstances around Brexit. This aspiration has been widely approved, including by the ICO.

During her appearance before the National Association of Data Protection and Freedom of Information Officers Annual Conference of 21 November 2016, the UK Information Officer Elizabeth Dunham confirmed upcoming guidance of the Article 29 Working Party on the GDPR. In fact, she stated that before the end of 2016, the Article 29 Working Party intends to provide instructions on the topics of the Data Protection Officers, the right to data

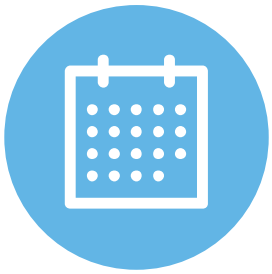
portability and the lead supervisory authority. For guidance on Data Protection Impact Assessments and the concept of risk, organisations will have to wait until February 2017.

She also stated that the ICO itself is developing its own guidance with regards to Big Data, consent and profiling. The ICO intends to seek the input of various stakeholders from different industry groups. In general, it considers it of utmost importance to adopt timely to the changes ahead.

Recent breaches and enforcement actions

- UK: A historical society was fined for a lack of adequate data protection policies to protect the personal data on personal devices when working from home. This resulted in a data breach, which prompted the ICO to impose a £500 fine.
- UK: The ICO fined a law services company £30 000 for making unsolicited marketing calls to people making use of the TPS (Telephone Preference Service).
- UK: An insolvency services firm received an enforcement notice from the ICO for transmitting direct marketing messages received through text.
- UK: The ICO launched an investigation into a recent hack of accounts of the National Lottery, after the gambling company denied being negligent.
- The Netherlands: Nike changed their app after receiving a warning about possible privacy violations after investigations by the Dutch DPA.
- The Netherlands: Chat service WhatsApp lost a court case in which it sought to abolish the measures taken by the Dutch DPA for not having appointed a representative on Dutch soil. The Court has now decided that the Dutch DPA has the right to request a local representative under Dutch data protection law, as the data of Dutch users has been used on Dutch smartphones without there being a transfer. As long as the chat service does not appoint a representative, it shall be subject to a fine of 10 000 euro a day, up to a maximum of 1 million.
- Germany: German DPAs will start auditing about 500 companies in respect of international data transfers with the goal of raising awareness.
- USA: The University of Massachusetts has agreed to a settlement with the US Department of Health and Human Services, Office for Civil Rights, having breached the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The University had been attacked by a malware program, which lead to the disclosure of electronically protected information. This uncovered both operational and technical security issues at the university.

Privacy events around the globe



CPDP Computers, Privacy & Data Protection

Burssels, Belgium, 25 – 27 January 2017
http://www.cpdpconferences.org/

The annual Computers, Privacy & Data Protection (CPDP) conference brings together academics, lawyers, practitioners, policymakers, industry and civil society to discuss legal as well as technological developments in data protection and privacy.

European Privacy Academy

Dolce La Hulpe, Belgium, dates below
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:

- 8 - 11 May 2017 and 18 September 2017
- 13 - 16 November 2017 and 5 February 2018
- 7 - 10 May 2018 and 17 September 2018

IAPP Europe Data Protection Intensive

London, United Kingdom, 13 – 16 March 2017
https://iapp.org/conference/iapp-europe-data-protection-intensive/

The Data Protection Intensive of the International Association of Privacy Professionals (IAPP) returns to London from 13 to 16 March 2017 and offers data protection professionals from around the world the opportunity to deep dive into today's critical data privacy topics and the coming challenges. The intensive is divided into a two-day training and workshop taking place as from 13 to 14 March. These practical sessions are followed by the actual conference on 15 and 16 March.

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