Privacy Flash – Issue 8

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

Privacy Shield challenged by Irish and French advocacy groups

On 16 October and 25 October 2016, the Privacy Shield has been confronted with two separate challenges, each of them seeking its annulment. While such a challenge was to be expected, it has come from a different corner than originally thought. It was not Max Schrems nor the Hamburg DPA that went to Court, but an Irish and a French advocacy group. On the Irish side, Digital Rights Ireland is taking the lead, trying to get the Privacy Shield annulled. On the French side, the advocacy groups la Quadrature du net, FDN and FFDN are questioning the Shield. In this claim, the most prominent elements are the bulk collection of data and the ombudsman not providing adequate protection.

Whether the claims will succeed is unclear, as a case for annulment requires a direct involvement of the applicant to be admissible. The Commission has acknowledged that it is aware of the complaint but hasn't commented. It is expected the cases will only be addressed after one year or more. It will be interesting however to follow the further developments and find out whether this Privacy Shield will be awaiting the same fate as its predecessor (see Issue 7 of the Belgian Privacy Flash).

ICO publishes code of practice to stimulate companies' transparency

On 7 October 2016, the ICO published a new code of practice that deals with the subject of how organisations should ensure transparency to individuals regarding the use of their personal data. The code got issued after an ICO survey had indicated that only one in four adults trusted businesses with their personal data and that too few organisations updated their privacy statements on a regular basis. With subjects such as Big Data, the Internet of Things and the digital single market becoming hot topics, it seems that awareness has increased, requiring privacy notices to be updated accordingly.

As such, the code recommends organisations to either produce a completely new privacy notice or work on the existing one by either further developing or evaluating it. Therefore, the code gives an overview of what is stipulated in the Data Protection Act and also looks ahead to the changes of the future GDPR and how to ensure transparency under the Regulation.

CNIL shares results on Internet sweep on connected devices

On 23 September 2016, the CNIL published the results of the Sweep carried out to look into the quality of information shared with users of connected devices. The purpose of the Sweep was to assess the level of security in data flows and the level of control allowing users to enforce their data protection rights. The sweep was conducted during the month of May as part of the so-called 'Sweep Day 2016' initiative, coordinated by the Global Privacy Enforcement Network. As such, it led to the following results with regards to the 300 tested devices:

- 59% does not provide clear and complete information on the topic of the collection and exploitation of the user's personal data
- 68% does not share any relevant information on the storage of personal data
- 72% fails to inform users of the ways to delete their data of the connected devices
- 38% does not provide contact details to allow users to get informed about the use of their personal data.

Furthermore, the results outlined that although the information given is often insufficient to properly inform the user whose personal data is being processed, users are usually satisfied with the amount of control they have over their personal data.

Next to the results, the CNIL also recommended best practices for these connected devices, one of those being the suggestions to always secure a smartphone or tablet either on the device itself or via a connected device, to use a pseudonym where possible and not to share data with people outside a trusted circle. Lastly, one should always delete personal data as soon as they become redundant.

Hungarian DPA shares 12-step guide to comply with the GDPR

On 11 October 2016, the Hungarian DPA published a guide for data controllers and data processors, explaining in 12 steps how to become compliant with the upcoming GDPR, enforceable as from 25 May 2018 (Issue 4).

The guide follows the recently published GDPR guidance issued by both the UK and Belgium as reported in Privacy Flash Issue 7. In the coming months, it is expected the DPA will issue additional instruments and guidelines for further assisting companies and organisations in preparing for the GDPR, since the current guide leaves a wide margin for interpretation.

EDPS publishes two opinions on Big Data and Personal Information Management Systems

The EDPS (the European Data Protection Supervisor: The DPA supervising EU institutions) has recently shared two opinions: One regarding Big Data and one on the protection of personal data using Personal Information Management Systems. The former one, published on 23 September, provided an update to the previous Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data, in order to be in line with the Digital Single Market Strategy.

As the Digital Single Market Strategy invoked an urgent need for the enforcement of digital rights, the EDPS recommended setting up a Digital Clearing House for enforcement in the EU digital sector, consisting of a voluntary network of contact points with regulatory authorities in charge of regulating the digital sector, both at national as EU level.

More specifically, the criteria to join the network would be twofold. On the one hand, the authorities should be willing to enhance their enforcement activities for the benefit of individuals' rights and welfare. On the other

hand, they should be open to sharing the necessary information within the boundaries of legal competences and confidentiality.

Secondly, the opinion also considered the need for an EU values-based common area on the web. Such a common area would entail an area where individuals can actually enjoy free services, without this being linked to any tracking or profiling. Following the opinion of the EDPS, such an idea is backed by several leading scholars and will stimulate the protection of privacy.

The other opinion published by the EDPS concerned user empowerment in managing and processing personal data. Via the Personal Information Management System (PIMS), individuals will have the opportunity to store their personal data in online storage systems and decide when and with whom to share it, with the aim of granting individuals greater control over their personal data. Giovanni Buttarelli, the European Data Protection Supervisor issued a press release on this opinion stating that:
"Our online lives currently operate in a provider-centric system, where privacy policies tend to serve the interests of the provider or of a third party, rather than the individual. Using the data they collect, advertising networks, social network providers and other corporate actors are able to build increasingly complete individual profiles. This makes it difficult for individuals to exercise their rights or manage their personal data online. A more human-centric approach is needed which empowers individuals to control how their personal data is collected and shared."

Article 29 WP shares conclusions from the Fablab discussions

On 7 October 2016, the Article 29 Working Party gave a comprehensive run-down of the various new GDPR concepts that were discussed during the so-called 'Fablab' workshop on 31 July, 2016. The purpose of the workshop, entitled "GDPR/from concepts to operational toolbox, DIY", was to provide assistance on how to timely and properly prepare for the GDPR.

Over 90 participants, including academics, representatives from the industry, civil society, associations and from Data Protection Authorities were present to help the Article 29 Working Party in developing best practices and guidelines to tackle priority issues such as data portability, certifications, Data Protection Impact Assessments, Data Protection Officers; which were already identified by the Working Party in its 2016 Action Plan.

Since several topics of the GDPR were clarified during the workshop, the Article 29 Working Party is planning to organise another Fablab Workshop in 2017.

Brexit might not affect data protection law in the UK

British Prime Minister Theresa May has recently announced that she will invoke article 50 of the Treaty of the European Union before the end of March 2017. This will kick-off a period of three years to allow the UK to adapt to the new situation caused by the Brexit. One element that has been thoroughly discussed is the European data protection law and what the consequences will be of the introduction of the General Data Protection Regulation in May 2018.

The main issue of the discussion is the 'resurrection' of the European Communities Act of 1972. This Act implies a transposition of all EU laws into UK law, but with the idea that it is up to the Parliament to either amend or cancel the law if it does not fully agree with the decisions made on European level.

Whether this Act will be relied upon for the GDPR however, remains unclear, as the GDPR will be in force before the end of the two-year transitional period started by the Article 50 invocation. Recent cases have shown a great need for some of the provisions provided within the regulation. The Yahoo case for example, enhances the idea that the 72 hour period to inform of a data breach would be a good solution for better transparency.

However, there are other elements in the European Data Protection law that the UK is reluctant to keep, such as its restrictive approach to data retention. As such, the UK has received great backlash for its proposed Investigatory Powers Bill, after the Data Retention and Investigatory Powers Act of 2014 was declared unlawful by the ECJ. Although some voices call for more privacy protective provisions to be added to the new bill, the questions remains whether this shall happen, once the watchful eye of the Court of Justice of the European Union (CJEU) disappears.

The Court of Justice of the European Union declares dynamic IP addresses to be personal data in Breyer decision

On 19 October 2016, the Court of Justice of the EU presented its opinion in the highly anticipated judgement of the Breyer case. In Breyer, a preliminary question was referred to the Court to seek its opinion on whether dynamic IP addresses can be considered as personal data. Mr. Breyer, who is a member of the "Pirate Party" did not agree with the German Federal Republic storing the IP addresses of its website's visitors in a log file. As such, these log files make a distinction between static and dynamic addresses. While it is a given fact that the former can identify a person, the dynamic IP addresses have been at the heart of several discussions.

Dynamic IP addresses have as characteristic that they differ every single time a new connection to the internet is made, which makes it difficult to use them as an identifier. The judgement of the Court clarifies once and for all that dynamic IP addresses are also considered to be personal data if they can be identified by 'legal means' (additional data) of third parties (ISP). This aligns with the opinion of the Advocate General in the case earlier reported on in Privacy Flash Issue 5, which also stated that such IP addresses are personal data and even named the same conditions thereto. Furthermore, it also confirms the opinion presented in a Working Document of the Article 29 Working Party published in 2009, where it explained why it considered the logged date, time, duration and dynamic IP addresses as personal data.

The judgement also dealt with a second question raised by the referring Court, this being the question whether a Member State was precluded from introducing a legislation that allowed the use of personal data without any consent for the purposes of facilitating and charging for access to online media services after terminating the access. In this respect, the CJEU

stated that it was indeed forbidden and that a general operability should not be considered a sufficient justification to do so.

Yahoo-case might become test-case for the US Security and Exchange Commission

The US Security and Exchange Commission, which enforces federal securities laws and regulates the electronic securities market in the US, has considered the Yahoo case as the ideal opportunity to bring up the issue of data breaches due to the extent of the breach, the public scrutiny and the lack of transparency. The case could be seen as infringing the SEC guidelines from 2011, which contain specific provisions on the topic of reporting a hack on publicly traded companies that could imply "a material adverse effect on the business".

Yahoo has generally been criticised for not having informed its users of a data breach that took place late 2014, resulting in possibly the largest data breach ever recorded. Until today, it remains unclear for how long Yahoo was already aware of this breach, as it only very recently admitted this breach to have taken place.

Article 29 WP letters to Yahoo and WhatsApp on possible data protection violations

On 27 October 2016, the Article 29 WP has shared two letters it has written to tech giants Yahoo and WhatsApp. While the first one addresses the aforementioned Yahoo-case, the second one focuses on the new Terms and Conditions of WhatsApp which allows it to share data with Facebook.

The Yahoo case, as explained above, concerns the big data breach of late 2014 where a very large amount of user data was obtained by hackers. In its letter, the Article 29 WP demands Yahoo to put in place significant resources to allow it to understand, communicate and address all elements of the data breach and inform the data subjects of the situation. It also takes the opportunity to highlight its new dedicated working group for enforcement action, which helps to take coordinated actions across several Member States. According to the Article 29 WP's letter, this group might look into the case very soon.

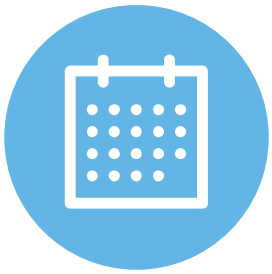
A second element pointed out in the letter is the recent positive answer of Yahoo to a request of the US intelligence agencies to search all of its customers' incoming emails with the aim of finding specific information. As such, the Article 29 WP seeks an explanation and justification for the massive data search, as it suspects it might not be in accordance with European data protection law.

In its letter to WhatsApp, the Article 29 WP is appalled about the fact that WhatsApp intends to share data with the 'Facebook Family of companies' even though it had previously declared that it would never do so. It points again to possible investigations by the new dedicated working group for enforcement and requests more information regarding the categories of data, the source of the data and the potential recipients of the data that WhatsApp intends to share, as to assess whether amendments made to the terms and conditions violate the European data protection legislation. WhatsApp has already declared its willingness to cooperate in the investigation.

Recent breaches and enforcement actions

- A British telecommunications company was fined £400,000 for failing to prevent a cyber-attack on its customer data. The company has done too little to protect the customers' information as the database was considered to be vulnerable and vastly outdated to hold back any malicious access. This fine is one of the biggest of ICO ever and falls just below ICO's limit of £500,000.
- A company was fined £20,000 by ICO for having sent out thousands of spam texts about loans.
- The UK DPA is continuing its investigation into British Showjumping, as to ensure that the agreed undertaking requirements signed in August 2015 are actively followed up.
- In the US, St. Joseph Health agreed to pay a settlement of $2,140,500 to the US Department of Health and Human Services, Office for Civil Rights (OCR) and adopt a comprehensive corrective action plan for having potentially violated the Health and Insurance Portability and Accountability Act of 1996 (HIPAA). Rather than awaiting enforcement, St. Joseph Health reported to OCR itself and arranged the settlement after an investigation by the OCR.
- The Dutch DPA has announced that it shall soon hand out fines following various investigations around data breaches with several companies. The DPA has shared that it has received almost 4000 cases of data breaches and is looking into some other investigations as well.
- A Dutch foundation has been considered to be in violation with privacy law regarding the protection of children and their parents, as information that is very personal is being shared.

Privacy events around the globe



European Privacy Academy

Dolce La Hulpe, Belgium, 13 – 16 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 November 2016 and 6 February 2017
- 8 - 11 May 2016 and 18 September 2017
- 13 - 16 November 2017 and 5 February 2018
- 7 - 10 May 2018 and 17 September 2018

IAPP Europe Data Protection Congress

Brussels, Belgium, 7 – 10 November 2016
https://iapp.org/conference/iapp-europe-data-protection-congress/

The annual Data Protection Congress of the International Association of Privacy Professionals (IAPP) returns to Brussels from 7 to 10 November 2016 and offers participants keynotes from prominent privacy professionals, as well as thoughts on the upcoming General Data Protection Regulation (GDPR) from prominent data protection regulators.

11th Annual Data Protection Practical Compliance Conference

Dublin, Ireland, 17 – 18 November 2016
http://www.pdp.ie/conferences/conferences-overview/82-11th-annual-data-protection-practical-compliance-conference

The Annual Data Protection Practical Compliance Conference is dedicated to divulge information on and prepare organisations for the General Data Protection Regulation. Next to the workshops, guests will have plenty of opportunity to network with other Information and Compliance professionals and advisors.

Conference on the General Data Protection Regulation

Mechelen, Belgium, 18 November 2016

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

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