Privacy Flash – Issue 10

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

European Commission unveils proposal for an ePrivacy Regulation

The European Commission published a proposal for a regulation on the confidentiality and privacy of electronic communications, set to replace Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (the "ePrivacy Directive"). The draft extends the current rules on privacy and data protection to all forms of electronic communications, regardless of whether they are publicly offered by a telecommunications provider or an "Over-the-Top" communication service (e.g. Skype, WhatsApp, Viber, Facebook Messenger).

The proposal reflects changes in consumer trends, with users replacing traditional voice telephony with functionally equivalent services like VoIP communications and instant messaging. Long excluded from the ePrivacy Directive, these services are now subject to confidentiality obligations (though also, in time, to potential derogations introduced by Member States setting out under which conditions such confidentiality may be waived).

The draft regulation is intended to complement the GDPR, to which it refers for a common set of definitions, rules on notification of data breaches, and the imposition of administrative fines of up to 4% of the annual global turnover. The definition of consent, still the main legal basis upon which the content of electronic communications may be processed, is now also consistent with the GDPR (i.e. an agreement that is "freely given, specific, informed and unambiguous (…) by statement or by a clear affirmative action").

Also revised was the controversial "cookie provision", often considered responsible for the ubiquity of cookie-banners in websites and for causing consent-fatigue amongst users. The new draft clarifies which types of cookies are exempt from consent and establishes new ways for users to define their preferred level of privacy (for example, through browser settings). Users are to be prompted every six months with the possibility of withdrawing consent.

Reactions to the proposal were varied. Telecoms called for more flexibility on the processing of personal data for secondary purposes and warned against overburdening communications providers who seek to develop competing products that rely on such information, such as mapping services. Other parts of the e-coms market, such as on-line advertisers, greeted the draft with "dismay", pinpointing the disastrous effects that the new rules can have on the advertising business model, without bringing any real added-value to users' privacy. On the other hand, consumer organisations heralded it as an opportunity to "confront the widespread problem of online tracking".

Though slated to apply from 25 May 2018, the proposed regulation will first need to run the gauntlet of the European Parliament and be approved by the EU Member States.

Privacy Shield in danger?

On 25 January 2017, newly inaugurated US President Donald Trump signed an Executive Order regarding the enforcement of US immigration laws, titled "Enhancing Public Safety in the Interior of the United States". While seemingly unrelated at first sight, it may have an impact on the future of the EU-US Privacy Shield, the "after Safe Harbor" framework which was agreed upon between the European Commission and the previous US administration last year to facilitate the transfer of EU personal data to the US.

Section 14 of the Executive Order states that: "*Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.*"

This section appears to be in direct contradiction with the Judicial Redress Act (JRA), which extends the core of the judicial redress rights that US citizens enjoy vis-à-vis US law enforcement authorities to the citizens of all EU Member States (except the UK and Denmark). The JRA does however fall within the remit of "applicable law" to which reference is made, as it was signed into law by President Obama on 24 February 2016, and is as such not directly impacted by this Executive Order.

The extension of redress rights under the US Privacy Act of 1974 to EU citizens was a key issue for the European Commission in the negotiations on the Privacy Shield. Any changes to the Judicial Redress Act or indeed the status of EU Member States as "covered countries" under the Act, may have an impact on the continued validity of the Privacy Shield in its current form. Countries can be removed from the list on initiative of the US Attorney-General, if the Secretary of State, Treasury Secretary and the Secretary of Homeland Security approve as well. In the US political system, all four of these functions are part of the executive branch, and thus of the Trump administration.

Article 29 WP publishes GDPR guidance on three key topics

On 13 December 2016, the Article 29 Working Party has adopted its first guidance on topics addressed in the GDPR. The guidelines touch upon three core requirements of the new Regulation that raise many questions relating to their implementation: the appointment of the Data Protection Officer (DPO); the right to data portability and how to identify the lead DPA in case of cross-border personal data processing.

Data Protection Officers (DPO)

With regards to the DPO function, the document follows the structure and content of the relevant articles of the GDPR (Article 37-39), which defines three cases in which the appointment of a DPO is mandatory.

Firstly, a DPO is mandatory in case it concerns a public authority or body. It is left for the Member States to decide in which exact cases this applies.

Secondly, a DPO can become necessary when the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale. As this requirement is quite lengthy, the Article 29 WP has broken it down into different sections with regard to the key concepts.

It notably clarifies that the term "core activities" means primary activities of the organisation and those "inextricably" linked with these main activities. "Large scale" seems to be intended to exclude companies who have a small amount of data subjects, concern only a small volume of data being processed and are limited in their duration of processing or in their territorial application. Regardless of this indication provided by the Working Party, it seems to be at the discretion of the organisation again, whether or not their processing activities are considered to be of a "large scale". For "regular and systematic monitoring", the Article 29 WP appears to be eyeing the companies that perform profiling and tracking on a reoccurring or pre-organised basis.

Thirdly, a DPO will also be required if the core activities of a controller or processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences. The Working Party confirmed that this article should be read as "and/or", i.e. processing just one of the two categories of personal data can trigger the requirement.

In any case, a DPO shall perform the tasks laid down in Article 39 GDPR as a minimum. In this regard, it is important to note that a DPO shall not be in charge of Data Protection Impact Assessments, but shall only be expected to provide advice to the controller on its practicalities. In a similar sense, it is also not supposed to perform the record-keeping, but in practice, can help the controller in doing so.

Moreover, the Working Party recommends that organisations processing personal data create a documented assessment of whether or not they consider a DPO appointment to be mandatory, "unless it is obvious" that it is not mandatory. If an organisation were to voluntarily assign a DPO, the same requirements of the GDPR will apply, unless it is made clear to all stakeholders in all public communications that the function of this person is not that of a formal DPO under GDPR (but for example a CPO or Privacy Officer).

Data portability

The second guidance concerns the right to data portability. This right aims at increasing data subject's control over their own personal data, by obliging controllers to hand it back to them in a commonly used machine-readable form, or to transfer it directly to another controller.

The right to data portability applies to personal data *provided by* the data subject, where processing is based on consent or is necessary for the performance of a contract. The Article 29 Working Party interprets "provided by" more broadly than most industry observers expected, as it covers not only data that is "knowingly and actively" provided by the data subject, but also data that are "generated by and collected from the activities of users". Only "inferred or derived data", such as a customer's credit score, can be considered to fall outside the scope.

On the question whether data affecting Intellectual Property falls within the scope, the Working Party has confirmed that misuse of the right with the aim of uncovering e.g. trade secrets shall not be tolerated. However, it should also be highlighted that a potential business risk does in itself not qualify as sufficient reason for refusal. An important caveat pointed out by the Working Party is that the controller is obliged to respond to the request, regardless of whether this is a positive answer or not. It will only be allowed to refuse if it has legitimate reasons to do so.

Lead Supervisory Authority

The third guidance note delivered by the Article 29 WP, is the one concerning the designation of the lead supervisory authority. The lead supervisory authority shall be in charge of coordinating the operations of supervisory authorities when several EU Member States are involved, either because the controller/processor is established in several Member States, or because its activities are likely to substantially affect data subjects in more than one Member State.

To identify this authority, if it concerns a controller, the Article 29 WP has indicated a three step check, starting with the question whether the controller/processor has a single establishment in the EU. If so, the lead authority will be this of the central place of administration, if not, one has to ask whether the controller has EU headquarters. If yes, it should be asked what the decision capabilities of the headquarters are. If headquarters do not really have a decision-making power, then the lead authority may be determined on the basis of other more relevant establishments where processing takes place.

A similar idea is in place for processors, in the sense that the main establishment – being the place of the central administration in the EU – shall take the lead. If both a controller and processor are involved, it shall always be the controller who takes charge of the situation. Where a group of undertakings is involved, additional criteria need to be taken into account.

2017

These explanatory documents published by the Article 29 Working Party are only the first of an array of guidance long-awaited by business and public administration. In its Action Plan for 2017, the Party has committed to delivering on its 2016 Action Plan, including guidelines on certification and processing likely to result in a high risk, on Data Protection Impact Assessments (DPIA) and on administrative fines.

In the remainder of 2017, the Working Party plans to provide further information on consent and profiling, on transparency, data transfers to third countries and data breach notifications. It also intends to organise a new FabLab (the previous one referred to in our Issue 8), an interactive workshop to get the view of various GDPR stakeholders.

Be sure to check out our Guidance on the DPO later this month, including a comprehensive overview of the essential elements at stake when appointing a DPO.

New data protection rules for European Union bodies

Following on the heels of the GDPR and the recent proposal for an ePrivacy Regulation, the European Commission published a proposal for a regulation on the protection of personal data with regard to the processing carried out by Union institutions, bodies and agencies.

The text is the final piece in the core data protection framework of the European Union, and is intended to replace Regulation (EC) 45/2001 (which served a similar function in relation to Directive 95/46/EC).

Overall, the new regulation is an alignment with the provisions set out in the GDPR and, like the proposed ePrivacy Regulation, draws on the definitions and concepts in that instrument. The regulation also sets out the need to adopt a risk based approach and to conduct data protection risk assessments before carrying out processing operations.

The text clarifies the identity of data controllers and recipients in the context of processing operations carried out by Union institutions, bodies, offices and agencies. Also noteworthy is the reinforcement of confidentiality obligations in contractual relations with external processors.

The system of interactions between DPOs and the European Data Protection Supervisor (EDPS) created by the former regulation was found to be effective, despite concerns over the possible lack of authority and management support of the former. As a response to this situation, the proposal grants the EDPS increased supervisory and powers, including with regard to sanctions.

One point of interest in the future will be the interaction between the proposed Regulation and the right to access documents of the European Parliament, Council, and Commission. It remains to be seen whether the reinforced, GDPR-class data subject rights of this Regulation will alter the way documents from Union bodies are accessed. In the past, complex cases have arisen from the refusal to disclose public information based on the argument that it contained personal data.

NIST updates Cybersecurity Framework

The US National Institute of Standards and Technology (NIST) has updated its Framework for Improving Critical Infrastructure Cybersecurity (more commonly known as the Cybersecurity Framework).

The draft is a response to feedback received since the release of Version 1.0 in 2014, and includes, amongst others, a new section on cybersecurity measurement, expanded context on the use of the Framework and refinements related to identity access management and access control (authentication, authorisation, and identity proofing).

First published in 2014, the Cybersecurity Framework is a set of best practices from a number of standards bodies and industry contributors. While originally intended for operators of critical infrastructures, its guidelines have been implemented across organisations of all sizes and sectors.

Belgian DPA announces public consultation concerning Data Protection Impact Assessments (DPIA)

The Belgian DPA has recently published a recommendation on Data Protection Impact Assessments, in anticipation of the Article 29 WP guidance due to be published in February 2017. As such, it tries to provide an answer to the most common questions on the topic of DPIAs. Besides presenting its insights, it has also opened up the conversation to other stakeholders, to gather their advice and suggestions, with the intent of publishing a final version afterwards.

According to the DPA, the obligation to conduct DPIAs should be viewed in light of two other elements of the GDPR: accountability and the risk-based approach. Where the former focuses on being able to prove such compliance, the latter entails taking a scalable and appropriate approach to compliance, in line with the risk that the processing poses for the rights and freedoms of data subjects.

In general "risk" seems to be a very key topic in the Belgian DPA's discourse. Following article 35.1, a DPIA shall be mandatory when the processing is *likely to result in a very high risk*, which is explained by the Belgian DPA as being likely to lead to significant adverse consequences for the rights and freedoms of individuals if no suitable security measures are taken. The only exception shall exist when the processing takes place based on a legal obligation or for the general good.

An important distinction made by the DPA in this regard is the difference between an inherent risk and a residual risk. An inherent risk shall refer to the probability of a negative impact taking place without the right cautious measures, whereas a residual risk shall mean the risk of such negative impact taking place, regardless of having taken the correct measures.

The DPA further took up the task assigned to it in the GDPR (Article 57) of drawing up a list of processing activities for which a DPIA is required. Examples from this list include the use of biometric data for identification purposes, the creation of risk profiles, and profiling activities on a large scale. In addition, the DPA also took the opposite approach and defined a list of activities for which a DPIA is not required, such as processing activities exclusively for the purpose of personnel administration. However, the Privacy commission emphasised that the existence of the lists does not in any way exempt controllers from the obligation to perform risk assessments and engage in appropriate risk management.

Whether this guidance will change following the input from stakeholders remains to be seen. In any case, the public consultation shall remain open until 28 February 2017.

Draft Swiss Data Protection Act published

On 22 December 2016, the Swiss Federal Department of Justice and Police published a new Data Protection Act. The Act anticipates the application of the GDPR and aims at maintaining Switzerland's status as an adequate country for international data transfers in the GDPR universe. It enhances the strength of the Federal Data Protection Information Commissioner, with administrative fines reaching up to 500,000 CHF and aims to improve data subject rights regarding their control over their data.

In other news, the Swiss government has also announced its own Privacy Shield agreement with the US. It considers this close relatedness of utmost importance, as it "*guarantees the same general conditions for persons and businesses in Switzerland and the EU/EEA in relation to trans-Atlantic data flows*". The Switzerland-US Safe Harbour framework was discontinued as well following the Schrems case that led to the invalidation of its EU namesake.

The Netherlands publishes draft of GDPR Implementation Law

The Dutch government introduced its proposal for a GDPR implementation law on 9 December, which will revoke the current Dutch Personal Data Protection Act. The new law, once adopted, is expected to increase harmonisation, improve the protection of personal data and enhance the free flow of data within the EU. It appears that the Dutch Government has decided to stick closely to its previous law in the areas in which the GDPR left room for deviations by Member States. A good example of this are the exceptions concerning the processing of health data, where the contents of the original Dutch Personal Data Protection Act have been fully transposed in the new law.

The Dutch government has opened this draft up for consultation of the various stakeholders until 20 February. All responses will be published.

Tele2 Sverige case limits national retention laws

The ECJ has recently provided its long-awaited judgement in the case of Tele2 Sverige, which centered around the question whether mass data retention was still possible after the invalidation of the Data Retention Directive in the Digital Rights Ireland Case.

In its judgment, the ECJ continues to condemn general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. However, it also considers a limited exception for Member States in their application of regional law if they abide to strict conditions.

This includes that the retention can only occur for the purpose of fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, where there is no requirement that the data concerned should be retained within the European Union and only to the extent that the retention is targeted.

This conclusion seems to divert from the earlier opinion of Advocate General Henrik Saugmandsgaard, who stated that a general retention obligation could be feasible under EU law, if limited by strict requirements. Under this new judgement, a general retention obligation shall no longer be feasible.

US Government seeks to join Digital Rights Ireland Privacy Shield case

The US Government has sought to intervene in the case of privacy advocacy group Digital Rights Ireland against the Privacy Shield, a case which was further explained in our Issue 8. This intervention reminds a lot

of the recent case of the Irish DPA against the Model Contracts, where the US also requested the right to join the proceedings.

However, the US is not the only country who was applying to take part, as France, the UK, the Netherlands, Germany and Czech Republic have all made a similar plea as well. Furthermore, Microsoft and Business Software alliance, both of which heavily support the Shield, have also shown interest in joining the proceedings.

Regardless of the parties' eagerness to become an amicus curiae to the case, it will first be up to the European Commission to decide whether Digital Rights Ireland has enough grounds to approach the European Court of Justice directly.

Dutch DPA assesses one year of data breach notifications

The Netherlands has introduced a mandatory data breach notification in early 2016, even though data breach notifications will only become mandatory for the whole of the EU in May 2018, when the GDPR starts to apply.

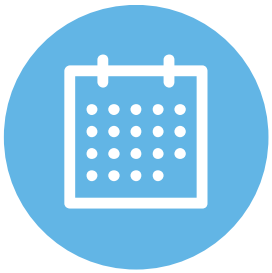
Now that the first year of this new obligation has passed, the Dutch DPA has provided insights into its statistics, which appear to be fairly high. Over 5,500 breaches were notified, 4000 of which were given a closer look. On this basis, over 100 organisations received a warning. In a few tens of cases, a deeper investigation was started by the DPA.

Interestingly, the sectors where most breaches took place were healthcare, financial services and public administration. According to the DPA, this was to be expected, as these sectors are known to process large amounts of data. In this assessment, the Dutch DPA also shared its appreciation for the clear increase in awareness this past year. It noticed a great influx of hints of possible infringements by data subjects, which also led to more investigations.

Recent breaches and enforcement actions

- The Dutch DPA has threatened with a penalty payment to foundation Abrona, specialised in providing disability care services, for violating privacy law concerning the sickness leave of its employees. Abrona has requested summary proceedings before national court, where its plea for suspension of the payment has been declined.
- After an investigation by the ICO, the Royal Society for the Prevention of Cruelty to Animals and the British Heart Foundation have been given a £25 000 and £18 000 penalty for screening their donors to target them for more money.
- A multinational general insurance company has been fined £150 000 by the ICO for losing personal data belonging to almost 60,000 customers.
- Another fine has been handed out by the ICO to a Bognor Regis firm for calling people registered with an opt-out service for telemarketing calls. The firm has been ordered to pay £40 000.
- A former agency admin worker of a mental health and learning disability NHS Trust has been prosecuted for looking into the sensitive medical records of people in her social circle, without having received their consent. She was given a fine of fined £45, was ordered to pay costs of £405.98 and a victim surcharge of £20.
- Two dating sites have been fined €10 000 and € 20 000 respectively by the CNIL (French DPA) for not having requested explicit consent when processing sensitive data.
- The FTC and dating site AshleyMadison have come to a settlement after the 2015 data breach. The site will implement a data security program, and pay a fine of $1.6 million.
- The US Department of Health and Human Services' Office for Civil Rights settles first HIPAA enforcement action for $475 000 with a large home health company for a breach of unsecured protected health information.
- Twelve institutions have been fined by the US Financial Industry Regulatory Authority (FINRA) for failing to protect customer records from alteration in accordance with federal securities laws and FINRA rules.

Privacy events around the globe



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 and offers data protection pros 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.

Global Privacy Summit 2017

Washington DC, USA, 17-20 April 2017
https://iapp.org/conference/global-privacy-summit/

The Global Privacy Summit returns to DC in April 2017, bringing together perspectives from around the globe for in-depth discussion and gold-standard education, big-picture inspiration and valuable connections. This conference is where privacy professionals come together every year to explore the answers, to synthesise a thousand views and see the way forward. The Summit starts with a two-day Training and Active learning on 17 and 18 April, followed by a conference on 19 and 20 April.

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