Deloitte.

Switzerland | Cyber Risk Services | Issue 4, May 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 4, May 2016

Highlights

European Data Protection Reform

European Parliament formally adopts the GDPR.

After four years of negotiations, the European Parliament in plenary session gave green light to the General Data Protection Regulation (GDPR) on 14 April 2016. The GDPR will enter into force 20 days following the publication in the Official Journal of the European Union. We hope to include the exact date in our next issue. The Regulation will replace the former 1995 EU Data Protection Directive and create a unified data protection law that will apply directly across all 28 EU Member States after a two years implementation period.

The GDPR wishes to streamline the data protection regime in Europe by imposing high standards and uniform rules that strengthen consumer rights and boost European competition.

Core points of the new regime

The key changes to the European data protection landscape that will have a major impact on businesses include:

- **Broader territorial scope**: The GDPR will not only apply to processing activities of data controllers and processors established in the EU but also to those that are not established in the EU but whose activities consist out of targeting data subjects in the EU.
- **Enforcement**: Under the new Regulation, Data Protection Authorities (DPAs) have investigative, corrective, advisory and authorisation powers. They are entitled to impose administrative fines ranging between 2 to 4% of the groups worldwide annual turnover of the preceding financial year or EUR 10 to 20 million, whichever is higher for infringements of data subject rights, non-compliance with an order of the DPA or the obligations of the controller and processor.
- **Accountability**: Contrary to the former DPA registrations, the GDPR imposes obligations to the controller as well as the processor to adopt technical and organisational measures such as privacy policies, appropriate security measures, maintenance of records of data processing authorities and performance of privacy impact assessments. Companies will have to appoint a Data Protection Officer in certain cases.
- **Expanded definitions**: The GDPR expands the definition of personal data to location data, IP addresses, online and technology identifiers. Pseudonymous data is defined as data that does not allow for identification of data subjects. Furthermore sensitive data now also includes genetic and biometric data.
- **Data subject rights**: The Regulation reinforces the rights that existed under the current regime (access, rectification, deletion, objection to the processing) and introduces the rights to erasure, restriction of the processing, data portability and the right not be subject to data profiling.
- **Consent**: The requirements for obtaining a valid consent have been spelled out more clearly, also focusing on the ability of individuals to distinguish a consent. The GDPR also introduces a special regime for children under the age of 16.
- **Data breach notification**: Controllers will be required to notify data breaches to the DPA within 72 hours after becoming aware of the breach and to the affected data subjects

without undue delay when the breach is likely to result in a high risk for the individual's rights. Processors are to report to the respective customer-controller.

- **One-stop shop**: When a company carries out activities in more than one European country, the Regulation introduces a one-stop shop mechanism allowing the DPA of the main establishment to act as the leading DPA, supervising all the data processing activities throughout the European Union. This mechanism facilitates the interaction for data controllers and processors with one lead DPA while the other DPAs still have a say on the level of cross-border operations through the consistency and cooperation procedures under the GDPR.
- **International data transfers**: The rules on data transfers outside the EU and EEA remain largely the same but are now all embedded in law (including Binding Corporate Rules and Standard Data Protection Clauses). Approved codes of conduct and certifications are new tools, still to be developed.

Links

- European Commission press release
- Official text of the GDPR in all official languages

EU-US Privacy Shield

Art. 29 WP issues opinion on the EU-US Privacy Shield

On 13 April 2016, Article 29 Working Party (hereafter the "Working Party") released its Opinion on the EU-US Privacy Shield following the publication of the draft Privacy Shield adequacy decision by the European Commission on 29 February 2016. As explained in our previous issue, the Privacy Shield seeks to replace the former Safe Harbour framework which was declared invalid by the European Court of Justice last year in the so-called Schrems case for not providing an adequate level of protection for the transfer of personal data out of the European Union. In addition to the Opinion, the Working Party also published a working document setting out essential guarantees for interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data.

The opinion of Article 29 Working Party is twofold. On the one hand, the Working Party welcomes the new framework as a significant step forward from the old Safe Harbour by stating that the shortcomings it had identified in April 2014 were addressed by the Privacy Shield negotiators. On the other hand, it stresses the lack of clarity and complexity of the new mechanism and issues concerns on both the commercial aspects and the possible derogations to the principles for national security, law enforcement and public interests purposes.

Key points of the new mechanism

- Strong obligations on companies handling EU citizens' personal data, and robust enforcement and monitoring by the US Department of Commerce and the US Federal Trade Commission.
- Clear safeguards and transparency obligations on US government access to personal data and assurance for the respect of the principles of necessity and proportionality.
- Effective protection of EU citizens' rights with several redress possibilities in front of the Department of Commerce, Federal Trade Commission, an independent Ombudsperson and the installation of an alternative dispute resolution mechanism that is free of charge. Furthermore companies will be given deadlines to respond to complaints.

From a commercial point of view

The Working Party is not convinced that the Privacy Shield offers an equivalent level of protection to the data subjects from a commercial point of view since certain key European data protection principles are not laid down in the draft adequacy decision and the annexes or have been replaced by inadequate notions:

- First and foremost the **data retention principle** is not mentioned in the framework and cannot be interpreted from the purpose limitation and data integrity principle.
- Secondly the Working Party demands more clarity on the application of the **purpose limitation principle**.
- Thirdly since the Privacy Shield will also be considered as a mechanism for transfers outside of the US, it should be ensured that **onward data transfers** from a Privacy Shield company to a third country recipient provides for an equivalent level of data privacy protection and cannot escape from the EU data privacy principles.
- Finally the proposed **redress mechanism** is considered as being too complex for data subjects to be applied in practice by EU data subjects. The Working Party urges for more clarity on the various recourse procedures and demands that the Data Protection Authority (DPA) can be considered as the natural contact point for data subjects.

In respect of the national security level

Notwithstanding the fact that the Privacy Shield offers increased transparency on the access to personal data that is processed for national security and law enforcement reasons, the Working Party stresses that the new mechanism does not exclude massive and indiscriminate collection of data stemming from the EU. The Working Party is furthermore concerned that the position of the Ombudsman – i.e. redress mechanism to protect the data subject's rights with regard to US intelligence services – is not sufficiently independent and does not possess the most adequate powers necessary to exercise its task efficiently.

Conclusion

The concerns expressed by the Working Party in its opinion and the working document urge the European Commission to take the above stated points into account in order to improve the draft adequacy decision and to safeguard that the principles of the Privacy Shield provide the same level of protection as in the European Union.

Even though the opinion of the Working Party cannot be considered as having binding effects, it is still highly persuasive as its members are representatives of national DPAs of each European Member State. If the European Commission decides to continue finalising the

proposed adequacy mechanism, they still have to consult with the committee composed of representatives of the Member States. In the meantime the Working Party has stated that data transfers to the US under the existing mechanisms i.e. Binding Corporate Rules or Standard Contract Clauses remain valid.

E-Privacy Directive

On 12 April 2016, the European Commission issued a public consultation to revise Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (i.e. the e-Privacy Directive). The reform of the directive is launched in order to assess the need to broaden the scope of the directive which currently only applies to traditional telecom providers, to assess the consistency between the e-Privacy Rules and the GDPR and finally to enhance secure and confidential communications throughout the European Union. The consultation aims at gathering views of all relevant stakeholders on the proposed reform and will be open until 5 July 2016.

Turkey adopted law on the protection of personal data

After 10 years of discussions, the Turkish Parliament enacted Turkey's first comprehensive data protection law on 24 March 2016. It has entered into force on 7 April 2016. The new law is inspired by the EU Privacy Directive, using very similar data protection principles. A personal data protection authority will be established to supervise compliance. The new law also imposes restrictions on transfers to third parties and to transfers outside of Turkey (applicable from October 2016), lays down a breach notification obligation to the DPA and data subjects, and imposes registrations to the DPA. Fines of up to 1 million Lira (about 300,000 EUR) are possible. Organisations with affiliates in Turkey should assess the impact of the new law and determine which actions are to be taken and by when.

2016 global privacy sweep initiative

On 11 April 2016, 29 DPAs announced their participation in the 2016 global privacy "sweep". This initiative is being coordinated by the Global Privacy Enforcement Network and includes an

investigation into practices of internet connected devices (e.g. internet of things devices, smart metering systems, health devices, etc.). The objective of the initiative according to the Privacy Commissioner of Canada is to "*increase public and business awareness of privacy rights and responsibilities, encourage compliance with privacy legislation, identify concerns that may be addressed through targeted education or enforcement and enhance cooperation among privacy enforcement authorities*". The outcome will be published in September 2016. In the meantime the DPAs are free to initiate enforcement measures for companies that do not comply with the findings of the "sweep".

New Information Commissioner in UK

On 22 March 2016, Elizabeth Denham was put forward by the UK government to become the new Information Commissioner. Before officially getting this status, Elizabeth is to be heard by the Culture, Media and Sports Select Committee, and be approved by both the Privacy Council and Her Majesty The Queen. This will likely be a formality since the UK government already announced that Ms Denham will replace the current Information Commissioner Christopher Graham this summer.

Dutch DPA prohibits employers to process employee data collected through wearables

Recently, the Dutch DPA ordered two companies in the Netherlands to stop processing health data of their employees which were collected via a bracelet designed to track the steps of their respective employee. One company also received the sleep patterns. The Dutch Authority argued that the collected data (i.e. sleep pattern, amount of steps) was to be considered as sensitive personal data and thus it was illegal for the employer to process them even though the employees had given consent. The DPA argued that an employee is not in the position to give a valid "freely given" consent. The employer, nor the staff members or the supplier of the device acting on behalf of the employee cannot process the data, not even if this is done in an anonymous manner. The DPA argued that employers can give a smart bracelet to employees but cannot link conditions to its use. The employee can chose to share the data with the supplier, for example through the supplier's portal, and can chose to share it onward with friends or colleagues, but not with its employer, its supervisor or any staff member acting on behalf of them.

Dutch DPA accepted BREIN's processing of personal data for IP infringement by BitTorrent users

BREIN, a Dutch association that fights intellectual property fraud, has received the approval of the Dutch DPA to process personal data of BitTorrent users, such as their IP addresses and users names to investigate the involvement of people in unauthorised exchange of copyrighted works. BREIN communicated that it would take adequate steps (organisational measures and clear data retention periods) in order to effectively protect the user's personal data and to only retain the data of users for whom strong suspicion exists of breaching the copyright law.

Dutch DPA publishes policy on data of sick employees

The Dutch DPA has published its policy relating to the processing of personal data of sick employees, covering the whole chain of administration, ranging from the employee itself, his employer, physicians, reintegration, social security and insurances. The policy dives into the various phases in the labour relationship, starting from the application procedure, the reporting of illness, the support and re-integration of sick employees.

Italian DPA publishes new manual on privacy and debt collection

The Garante, the Italian DPA, has published a new manual on the proper processing of personal data in debt collection. The manual can be downloaded from the Garante's website.

EDPS guidance on information security risk management

The European Data Protection Supervisor (EDPS) has published guidance on “Information Security Risk Management” (ISRM) on 21 March 2016. Its main objective is to provide European institutions with practical steps on how to comply with article 22 of Regulation 45/2001 (the “privacy act” applicable to EU institutions). The guidance takes into account generally accepted good practices on the matter of ISRM and wishes to help European institutions in creating a digital environment which is secure and trustworthy for the information they use.

EDPS: Case law overview

On 16 March 2016, the EDPS published an overview of the most relevant data protection case law for the period of 1 December 2014 up to 31 December 2015.

European Parliament refuses to vote on PNR

As mentioned in one of our previous Privacy Flash issues, a new proposal was made to create an EU Directive that would oblige air carriers that operate flights between a third country and an EU Member State to hand over the Passenger Name Record (PNR) data to the competent Member State authorities. The Member States would then share alerts created based on PNR data and have the right to request PNR data from one another in support of specific investigations. The provisional agreement on the EU PNR proposal was approved by the LIBE Committee of the European Parliament last December and this proposal should have been presented to the plenary session of the Parliament in order to be voted. However, on 7 March 2016, some MEPs refused to present it to the plenary meeting stating that “*they fear a vote on PNR may allow member states to abandon the personal data protection package they have promised as a counterweight to the new surveillance powers*”.

Right to be forgotten requests to be directed to Google Inc., not Google Spain

On 15 March 2016, countering the Spanish DPA's resolutions, the Spanish Supreme Court decided that the right to be forgotten does not apply to Google Inc.'s Spanish affiliate. According to the Supreme Court Google Spain, S.L. only provides advertising services. Since it does not determine the means nor the purposes of the processing, Google Spain cannot be considered as a data controller. This judgment however doesn't change much to the basic rule; from now on, the data protection cases will have to be brought in front of the parent company, Google Inc.

Binding Corporate Rules of Starwood Hotels and Resorts approved

The EU cooperation procedure for the approval of the Binding Corporate Rules of Starwood Hotels and Resorts has been completed. Starwood is one of the leading hotel and leisure companies in the world, operating under several brands including Sheraton, Westin and W. The Belgian DPA acted as lead authority. The full list of companies for which the EU BCR cooperation procedure is closed can be found on the data protection website of the European Commission, DG Justice.

Recent breaches and enforcement actions

- On 16 March 2016, Jan Philipp Albrecht won an MEP award for his outstanding achievement as rapporteur on the GDPR.
- On 17 March 2016, ICO fined a boiler firm in Britain £180,000 for initiating more than 2,000,000 unwanted calls from April until July 2015. The firm had recorded a promotional message and people were called without having given their consent.

- A British politician has received a fine of £5,000 for having instigated 35,000 recorded nuisance calls without having the consent of the people contacted. The calls were performed in order to convince people to support his nomination as mayor of London.
- On 21 March 2016, after receiving 5,535 complaints, the ICO has fined a firm for having performed almost £2,500,000 automated calls for marketing reasons without having any prior consent. The ICO had already warned the firm in August to be compliant with the Privacy and Electronic Communications Regulations, and had also asked the firm to provide proof that it had effectively received the consent of the recipients – which it couldn't provide. Because the firm didn't cease the automated calls (while claiming the contrary) and because of the huge amount of complaints, the ICO decided that the infringement was deliberate and serious enough to impose a penalty to the firm.
- On the same day, the ICO imposed another fine to a company for which 167 complaints were lodged for unsolicited calls. Since this infringement was negligent and serious enough, the ICO issued a fine of £50,000.
- On 24 March 2016, Google got fined EUR 100,000 by the French DPA (CNIL) for lacking to submit a coherent de-listing service.
- On 24 February 2016, a German court ruled that a website, using the "Like" button without informing the visitors that their IP addresses were transferred to Facebook, infringed German data protection law. The website was asked to notify the visitors of this transfer, to obtain their consent and to explain them clearly that it is possible for them to revoke their consent.
- The Bundeskartellamt in Germany has initiated proceedings against Facebook for the abuse of its dominant position by breaching data protection law. Moreover, Facebook is suspected to impose unfair terms and conditions on its users. The President has stated that "*it is essential to (…) examine under the aspect of abuse of market power whether the consumers are sufficiently informed about the type and extent of data collected. Users are not sufficiently aware what they are committing to, when accepting these terms and conditions.*"

Privacy events around the globe

EDPS – Civil Society Summit

Brussels, Belgium, 16 June 2016
https://secure.edps.europa.eu/EDPSWEB/edps/cache/offonce/EDPS/Events

On 16 June 2016, the European Data Protection Supervisor, together with the civil society organisation, will discuss the current state of data protection in the EU focusing on the

implementation of the GDPR and the directive on data protection rules for the police and criminal justice, the review of the e-Privacy Directive and the Privacy Shield.

Cyber innovations for financial services - Defending against ever-changing threats

Deloitte Academy, Zurich, Switzerland, 30 June 2016
Register for the event

The event addresses how financial services organisations can adapt to managing new and changing threats. Few areas are as dynamic and fast changing as cyber security. Beyond the usual arms race between attackers and defenders, regulators have started to weigh in and set expectations on how financial services firms are to manage their cyber risks. The topics will include recent developments starting with cyber regulation and the role audit can play in protecting your enterprises, followed by presentations on cyber innovation and the potentially game-changing approaches that financial services institutions can pursue to better protect themselves.

For further information on the event please contact Ms. Isabelle Buecheler via email or phone at: +41 58 279 77 71.

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, etc.

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 is focused to put privacy on the agenda in the Arab, Muslim and African regions.

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