Privacy Flash – Issue 7

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

DPAs comment on Privacy Shield

As reported in Privacy Flash issue 6, the European Commission adopted the EU-US Privacy Shield framework with an adequacy decision on 12 June 2016. By notifying the Member States, the new framework for EU-US personal data transfers entered into force immediately. The adoption of the Privacy Shield marks the return to normalcy for transatlantic data transfers after the previous Safe Harbour framework was invalidated by the European Court of Justice in October 2015. As of 1 August 2016, companies are again able to self-certify with the US Department of Commerce, which operates the Shield.

The European Data Protection Authorities were positive about the amendments made to the first draft of the Privacy Shield. Nevertheless, they remain sceptical with regards to the commercial aspects and the access by U.S. public authorities to data transfers stemming for the European Union. According to the DPAs, the Privacy Shield lacks provisions on automated decision-making and on the right to object to data processing. Furthermore they urge for clarification on the applicability of the provision to data processors. Additionally less strict guarantees should be enacted on the independence and powers of the Ombudsperson.

According to the Chairwoman of the Art. 29 Working Party, the adequacy of the EU-U.S. Privacy Shield will not be challenged in its first year. In May 2017, the European Commission has scheduled a mandatory review of the adequacy of the Privacy Shield.

EU ePrivacy Directive under review

On 11 April 2016, the European Commission launched a public consultation to evaluate and review Directive 2002/58 on privacy and the electronic communication sector. The said Directive, commonly referred to as the ePrivacy Directive (ePD) was adopted with a view to harmonise national rules in relation to the processing of personal data in the electronic communications sector. The recent adoption of the General Data Protection Regulation (GDPR) as well as the rapidly changing technological landscape have inspired the European Commission to review the ePD.

As mentioned in Privacy Flash issue 4, the reform of the Directive was launched in order to assess the need to broaden its scope, which currently only applies to traditional telecom providers, as well as 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 aimed at gathering views of all relevant stakeholders on the proposed reform and was open until 5 July 2016. The objectives of the ePD's review are fourfold:

- Ensure consistency between the ePrivacy rules and the General Data Protection Regulation
- Update the scope of the ePD against the background of the new technological evolutions and market reality
- Increase security and confidentiality of communications
- Address conflicting enforcement and improve harmonisation across Europe

On 25 July 2016, the Article 29 Working Party and the European Data Protection Supervisor issued opinions on the ePD reform. Although these opinions are not binding in nature, their importance are considerable since they are an indication of how Data Protection Authorities will interpret the legal framework and how they aim to influence the reform of the ePD.

Art. 29 Working Party recommends the European Commission to:

- **Scope**: Extend the scope of the ePD to cover new types of telecom services ("over the top services") such as Internet telephony (VoIP), instant messaging, WhatsApp, webmail and messaging in social networks. Additionally the Working Party urges the Commission to clarify the meaning of "public electronic communications network", "electronic communications services" since they are often unclear and do not reflect the infrastructure of today's communication networks.
- **Confidentiality**: Apply the requirement of confidentiality to all publicly available networks and services (wired or wireless, public, privately owned or managed) such as Wi-Fi services offered in hotels, universities, trains and hotspots. Furthermore, the article laying down confidentiality should be revised to establish a general prohibition of the interception, surveillance, monitoring of the content of electronic communications.
- **Consent**: The prior consent of the user should remain key in the Directive, with regards to collecting metadata, content data and tracking techniques. Additionally, the Directive should refer to the GDPR provisions to ensure consistency.
- **Cookies**: The provision on cookies should be rewritten in order to be as technologically neutral as possible to cover tracking techniques used on smartphones and Internet of Things applications.
- **Direct marketing**: Revise the rules for unsolicited communications to ensure prior consent of the user for all types of unsolicited communications irrespective of the means used (e.g. mail, fax, text, video calls, etc.).
- **Deletion of data breach notification rules**: To avoid duplicate notifications given the GDPR's data breach notification requirements, the Working Party recommends deleting the current data breach notification rule from the ePD.
- **Enforcement**: Data Protection Authorities operating on the basis of GDPR should also be competent on ePD matters that involve personal data to promote harmonised sanctions and consistent enforcement.

The opinion of the EPDS closely relates to the Working Party's recommendations with regards to extending the scope, improve the protection of confidentiality of electronic communications, requiring prior consent for unsolicited communications, conditions for consent, etc.

The finalisation of the e-Privacy Directive reform will be expected by the end of 2016.

Russian data localisation update

As previously reported in our Belgian Privacy Flash issue 6, Russian's new data localisation requirement entered into force in September 2015. The amended data protection law now requires companies from all over the world collecting or processing personal data of Russian citizens to store these data on Russian territory. The entry into force followed a warning shot by the government's IT, telecom and media regulator Roskomnadzor, who briefly blacklisted the Russian-language version of Wikipedia in August.

In Russia, Roskomnadzor acts as the de facto Data Protection Authority. One of its task is to oversee the enforcement of the new data localisation rules, which seems to be initially aimed at Russian companies. According to reports, large foreign internet companies have been given until 29 August 2016 to comply.

On 1 September 2016, Roskomnadzor reported to the press on the progress made during the first year of enforcement. The regulator came to the overall conclusion that a big majority of the audited companies comply with the localisation requirement. The audits cover mainly industry "clusters" such as e-commerce platforms, recruitment agencies, insurance companies and others. Additionally, general monitoring activities are carried out in reaction to public complaints.

Since September 2015, 954 scheduled audits and 82 ad hoc audits were carried out. In the upcoming months another 470 audits are planned. The regulator identified about 1,822 infractions of which only 23 were related to the data localisation requirement. Next, another 8 infractions of the latter requirement were identified through general monitoring. The regulator has ordered to cease the infractions within a period of sixth months.

Furthermore the regulator detected frequent usage of the online register of data operators that violate the Russian data protection law. About 161 blocked websites have been listed in the register up to now. In addition, about 63,000 data operators have notified the regulator of the location of their databases in accordance with the legal requirement to notify databases containing personal data.

It is fair to say that the recent press release indicates that the Russian privacy regulator will proceed to enforce the data localisation requirement, mainly through audits. Instead of being fine focused, the main purpose of the regulator is to motivate companies to comply with the regulations in place.

WhatsApp's sharing of user personal data with Facebook under scrutiny of EU DPAs

On 25 August 2016, WhatsApp announced an update to its Terms of Service and Privacy Policy in order to allow user data to be shared with Facebook. Upon WhatsApp's acquisitions by Facebook in 2014, both companies were requested by the Director of the FTC's Bureau of Consumer Protection to update their privacy notices with the objective to inform consumers about the recent merger.

In the Frequently Asked Questions, WhatsApp sets forth the reasoning behind this update. The new Terms of Service and Privacy Policy were updated to help customers gain insight in the new WhatsApp features and services such as WhatsApp Calling, WhatsApp for web and desktop and end-to-end encryption, as well as their strategy to assist customers to communicate with businesses that use WhatsApp services.

Notwithstanding the fact that WhatsApp is now part of Facebook, both entities will continue to provide separate services. This however does not prevent personal data to be shared with Facebook and the Facebook family of companies for enabling better coordination and to improve the effective use of both companies' services.

The stated overall purpose for which information will be shared with Facebook is to allow both companies (1) to calculate more effectively unique users, (2) to more efficiently fight spam and abuse, (3) to suggest Facebook users better friend suggestions and (4) to provide them with more relevant ads.

Despite the possibility to opt out of the said data sharing with Facebook, the British DPA (ICO) is concerned about WhatsApp's initiative to share user data with Facebook for the purpose of carrying out targeted advertising. On 26 August 2016, Information Commissioner Elizabeth Denham stated: "The changes WhatsApp and Facebook are making will affect a lot of people. Some might consider it'll give them a better service, others may be concerned by the lack of control. Our role is to pull back the curtain on things like this, ensuring that companies are being transparent with the public about how their personal data is being shared, and protecting consumers by making sure the law is being followed. We've been informed of the changes. Organisations do not need to get prior approval from the ICO to change their approaches, but they do need to stay within data protection laws. We are looking into this."

On 27 September 2016, the Hamburg DPA (Germany) took a firm action by ordering Facebook to stop storing and using personal data from over 35 billion German WhatsApp users. The German DPA believes the German privacy law has been infringed by misleading consumers and not requiring explicit opt-in consent for the sharing. Facebook said it would appeal the order.

Art. 29 Working party and other European DPAs, such as the Belgian and the French are also looking with great vigilance to the announced changes.

Belgian State Secretary for Privacy intends strengthening of DPA

During a television interview on 12 September 2016, the Belgian State Secretary for privacy, Philippe De Backer, announced his intention to strengthen the powers of the Belgian Data Protection Authority , the Privacy Commission.

In his view, Data Protection Authorities (DPAs) should be empowered to sanction and impose fines onto companies which do not comply with the Belgian Privacy Act. He stated that fines will only be a last measure of redress. As a first step, DPAs should be more proactive. This would entail using the power to carry out privacy audits in a number of determined business sectors to check the current state of compliance with the requirements under the Privacy Act. Furthermore, the State Secretary highlighted the importance of raising privacy awareness amongst data subjects, especially in respect of their rights and obligations under the Privacy Act.

Belgian DPA issues 13 steps to comply with the GDPR

On 16 September 2016, the Belgian DPA (the Privacy Commission) issued guidance on how to prepare for the General Data Protection Regulation, which will be applied as of 25 August 2018.

The guidance was issued following requests from many businesses on the impact and applicability of the new Regulation. By following 13 proposed steps, data controllers and processors will be able to detect differences between the current Belgian Privacy Act of 1992 and the new Regulation enabling them to prepare for May 2018.

In the upcoming months, the Belgian DPA will issue additional guidelines and develop instruments for further assisting companies and organisations with their preparation.

In the meantime, the Belgian DPA advises companies to identify which provisions of the GDPR will have the biggest impact on their processes and to prioritise those when assessing compliance with the new regulation.

South Africa nominates data protection regulator

South Africa's National Assembly has nominated Pansy Tlakula on 7 September 2016 as the **Chair of the National Information Regulator** to enforce the Protection of Personal Information Act 2013 (POPI) and to nominate the members of the office.

The South African regulator's office works independently and can be held accountable by the National Assembly. Together with her co-workers, Pansy Tlakula will hold office for five years maximum with the possibility to be re-elected. The nomination will now have to be formally confirmed by the South African president.

The regulator will have investigatory and enforcement powers to (amongst others) issue large administrative fines and demand publication of data breaches.

Following the nomination of the regulator, certain rules of the POPI will have to be promulgated and the date of commencement of the Act will have to be made public. Companies will be given time to comply with the new rules and will not be held accountable for non-compliance for the 12 months post commencement date of the Act. Some voices state that the commencement date should be 24 May 2017, a year prior to the European General Data Protection Regulation becoming enforceable. This timeframe would allow companies to manage compliance with both the European regulation and the South African act.

The Philippines finalise implementing rules to the Data Privacy Act

In the Philippines, a comprehensive Data Privacy Act has been put in place since 8 September 2012. The latter Act mandated the establishment of a National Privacy Commission (NPC) empowered to supervise compliance with the Data Privacy Act and to issue rules (IRRs) regulating the implementation of the Act. Following a public consultation, the Implementing Rules and Regulations of Republic Act No. 10173 (IRRs) were published on 24 August 2016 and are enforceable as of 9 September 2016, 15 days after publication in the Official Journal.

The publication of the IRRs is to be considered a major step forward for the protection of personal data in the Philippines. The rules aim to establish a high level of protection and are based on those already implemented in other data protection regimes such as the GDPR in Europe and the Personal Information Protection Act (PIPA) in South Korea.

Some of the main concepts of the Data Privacy Act are listed below:

- The Act defines personal information as "any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual". Sensitive personal information are additionally protected. When processing sensitive data of over 1,000 data subjects, data controllers and processers are obliged to register the data processing with the NPC within a fixed period of one year.

- The material scope not only covers data controllers – those who determine the means and purposes of the data processing, but also data processors – those who act on the instructions of the data controllers. Also personal data not relating to Philippine residents is protected by this Act.
- Transparency, accuracy, legitimacy, proportionality are central principles under the Act.
- Private sector data sharing can only take place with the prior consent of the data subject.
- A data protection officer, compliance officer, or any other person has to be appointed by each person or body that processes personal data and will be accountable for the protection of privacy and security.
- Security measures including organisational, physical and technical have to be adopted taking into account the nature of the data, risks, size of organisation, complexity of operations, current best privacy practices and cost.
- Data controllers are obliged to notify the NPC of any data breach within 72 hours in the event of a real likelihood of serious harm to the data subject. Data breaches are sanctioned significantly including imprisonment from 1 to 3 years.
- In line with the GDPR, the Data Privacy Act also provides the data subject the right to be informed, to object, to access and to rectify personal data and to data portability.

State of New York proposes cyber security regulation for financial institutions

On 12 September 2016, the state of New York proposed a regulation requiring financial institutions such as banks and insurance companies to implement cyber security governance. One element of the proposed regulation includes the appointment of a cyber security officer with the task to oversee companies' cyber security program. Furthermore a written cyber security policy should be in place addressing a minimum number of fourteen cyber topics including incident response plans and the protection of data privacy. Companies will be required to notify the NYDFS of any material breach within 72 hours after discovery and carry out an annual risk assessment and penetration testing.

The timing of the proposal is not surprising, given the increased focus of the federal regulator, the Securities and Exchange Commission (SEC), on the financial industry's cyber security practices.

Earlier, the NYDFS has sent a survey to 200 regulated financial services institutions in order to gain a better understanding of the business' initiatives to fight cyber crime. Those surveys were summarised in the "Reports on Cyber Security" in the insurance sector on the one hand and the banking sector including third party service providers on the other hand.

Companies will be required to take steps to confirm that their current cyber security programs are in compliance with these new regulatory requirements. After publication in the New York State Register, the proposed cyber security regulation will be subject to a 45-day notice and public comment period.

Draft agreement between Canada and the EU on the transfer of passenger name record (PNR) data under fire

On 8 September 2016, Advocate General Mengozzi of the Court of Justice of the European Union issued an opinion on the compatibility of the draft PNR agreement between Canada and the EU with the European Charter of Fundamental Rights. The opinion can be linked to the Courts previous rulings in Digital Rights Ireland – declaring the Data Retention Directive invalid – and the Schrems case – declaring the Safe Harbour framework inadequate. Although AG opinions are not binding to the Court, they are of high importance for the Court and are mostly followed in its final judgement.

The PNR agreement was drafted in spring 2010 to gather passenger data of flights between Canada and the European Union. The transfer of data to competent Canadian authorities would serve to track and prevent terrorist attacks and other international crimes. The data collected covers amongst others passenger travel habits, payment information and dietary prescriptions revealing passenger's sensitive personal data such as health, religion or ethnic origin. Despite the fact that the draft agreement was signed on 25 June 2014, the European Parliament referred the agreement to the Court to verify compliance of the draft agreement with provisions of privacy and personal data as laid down in the Charter of Fundamental Rights.

According to the AG, the agreement is incompatible with the said Charter because (1) it concerns the use, retention and processing of sensitive data, (2) PNR data would be retained for a period of five years maximum without reference to the purpose, (3) Canada is able to process PNR data beyond what is strictly necessary and independently of the purposes as laid down the agreement and (4) there is an absence of adequate safeguards and mechanisms to supervise the subsequent transfer of PNR data to foreign authorities. In his opinion, the agreement should be amended to exclude the collection of sensitive data and to target only those persons who can reasonably be expected to be a suspect of international crimes and terrorism.

Recent breaches and enforcement actions

- The French Data Protection authority, CNIL, issued on 20 July 2016 a formal notice to Microsoft to seek compliance with the French Data Protection Act within the next three months. The notice was initiated due to Microsoft's new operating system - Windows 10 - that enabled excessive collection of personal data and the tracking of the browsing history of users without their consent. Several breaches were identified, related to - amongst others - proportionality, data security, registration requirements, cookie law and cross-border data transfers. Microsoft risks being sanctioned with a fine of possibly EUR 150,000 to EUR 3 million (under the new French Digital Republic Law).
- A car finance brokerage company was fined £30,000 by the Data Protection Authority in the UK, ICO, for sending out 65,000 unsolicited direct marketing text messages.
- A software firm has suffered a data breach by someone who used an internal login without being authorised. The ICO and the police are currently investigating.
- A local government body was fined £100,000 by the UK regulator for having left documents and files containing highly sensitive personal data in an abandoned building.
- A telecom provider was fined £1,000 after its appeal to the ICOs decision was dismissed by the Information Tribunal. The case concerned a failure to notify a personal data beach to the ICO within 24 hours, under the Privacy and Electronic Communications Regulation.
- Bluetrace, a technology company that develops Business Intelligence systems based on Wi-Fi and Bluetooth signals was issued penalties by the Dutch Data Protection Authority for gathering personal data of customers in the absence of providing prior notice.
- The ICO fined a debt management company for £40,000 for sending out unwanted marketing texts to data subjects.
- A marketing services company was fined £60,000 for making 1.6 million nuisance calls about market solar panels and green energy equipment.
- The ICO fined a local authority £100,000 for leaving behind files containing personal data in a disused building.

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
- 08 - 11 May 2016 and 18 September 2017
- 13 - 16 November 2017 and 5 February 2018
- 07 - 10 May 2018 and 17 September 2018

IAPP Europe Data Protection Congress

Brussels, Belgium, 7 – 8 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 on 7 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.

15th Annual Data Protection Compliance Conference

London, United Kingdom, 13 – 14 October 2016
http://www.pdpconferences.com/find-a-conference/82-15th-annual-data-protection-compliance-conference

This conference organised by PDP aims at providing data privacy professionals with the core tools and necessary information they need to have it applied in their daily practice.

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 aims at putting privacy on the agenda in the Arab, Muslim and African regions. The conference will be partially closed and partially open to the public. More information will be published in the coming months.

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 and prepare organisations on the General Data Protection Regulation. Next to the workshops, guests will have plenty of opportunity to network together with other Information and Compliance professionals and advisors.

Conference on the General Data Protection Regulation

Leuven, 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