Privacy Flash – Issue 11

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

Bavaria DPA sends GDPR questionnaire to 150 companies

To mark the half-way point of the two year period between the GDPR's publication and its application date, the Data Protection Authority (DPA) of Bavaria has distributed a questionnaire to 150 randomly selected organisations to help them assess how far they have come in their preparation for 25 May 2018.

In its press release, the DPA emphasised that new requirements in the areas of transparency and accountability pose significant challenges, as well as the introduction of new and strengthened data subject rights. In addition, the DPA clarified that the questionnaire should give companies an idea of how the DPA plans to use the new audit powers it will receive in a year's time.

German Data Protection Act approved

In anticipation of the application date of the GDPR in May 2018, Germany passed a new Data Protection Act on 12 May 2017. The new law makes use of the so-called "opening clauses" in the GDPR, which allow Member States to enforce stricter rules (e.g. regarding the mandatory DPO appointment) or to relax certain requirements (e.g. minimum age for valid consent).

As expected, Germany will continue to require organisations to appoint a DPO if they employ more than 10 persons who are permanently engaged in the automated processing of personal data. On the other hand, the German act goes beyond the GDPR in defining specific rules in the areas of video surveillance, consumer credit and creditworthiness. In addition, it creates rules allowing for the sanctioning of individuals, which could lead to personal liability risks for employees of data controllers.

German media have reported that the European Commission does not agree with the interpretation the German lawmakers have given to the opening clauses, citing comments made by the Justice Commissioner's head of cabinet at a data protection event in Berlin. Privacy activist groups as well as the German Data Protection Authorities have pointed out that the new German act undermines the GDPR's goal to harmonise data protection rules across Europe and noted that it creates legal uncertainty for businesses.

Introducing a complaints procedure under the Privacy Shield agreement

The Article 29 Working Party has recently shed light on the Privacy Shield by issuing rules of procedure and a template for submitting commercial-related complaints on 21 February 2017. The documents are intended to inform data subjects on how to notify a data breach under the Privacy Shield agreement.

European data subjects willing to submit a commercial-related complaint towards a Privacy Shield-certified company can use this template in order to bring the issue in front of their national Data Protection Authority. Although not a mandatory formality, the complaint form is a useful tool for submitting complaints in an efficient manner as it asks all the necessary questions needed to identify complaints and thereby facilitates complaint handling. Amongst others the form requires the data subject to provide the reasons for the data transfer, the alleged violation, the details relating to the certified company the claim is directed to and the relief sought.

Upon submission, the Data Protection Authority concerned will be responsible to appoint an Informal Panel of EU DPAs - in a timely manner and at least within two weeks after receiving the complaint or the referral - as the competent body to deal with the complaint as such. The panel is expected to issue a binding advice towards US companies as quickly as possible and at least within sixty days following the complaint. Complaints of Privacy-Shield-certified companies that are not willing to collaborate with the DPA panel's advice within twenty five days after receipt, will be forwarded to another body such as the US Department of Commerce or the FTC. The aforementioned authorities are entitled to issue enforcement actions in the event of deception or misrepresentation or otherwise could come to the conclusion that the company's agreement to collaborate with the DPA panel was seriously infringed and is consequently null and void. In that case, the Department of Commerce will amend the Privacy Shield list.

The rules of procedure are to be considered as a roadmap for the European DPA panel dealing with Privacy Shield complaints.

UK implementation NIS directive

Last year the EU issued the Network Information Security Directive, often referred to as the "cyber security directive" or "NIS". This legislation aims at enhancing the cyber resilience of the European single market and improving the overall level of cyber security across the European Union and its Member States by enforcing adequate security measures in order to protect citizens and business from all sorts of cyber threats.

The NIS directive emphasises on improving risk management strategies especially on critical infrastructure (banking, healthcare, energy and transport) and digital service providers (online marketplaces, search engines and cloud services) as these pose a significant vulnerability if risk is not managed appropriately. Services that process a large amount of sensitive data, be it personal information or not, are considered top priority because they are the cornerstones of modern society.

The cyber security directive, along with General Data Protection Regulation, will come into force in May 2018. This means that business and institutions should already have their eyes on these two legislations as they imply a serious impact on different critical domains and could impose significant penalties.

Despite the Brexit and the current approach to encourage businesses to manage their own risk as it is of the business best interest, the UK will most likely implement the NIS directive. The government has confirmed in January that it will set out "the detailed scope and security requirements for NIS implementation in 2017". The statement provides clarity in the light of the current developments and proves the awareness on the increasing cyber threats and the measures accompanied with them.

Spanish DPA publishes GDPR Guidelines

The Spanish Data Protection Authority (Agencia Española de Protección de Datos, or AEPD) has published a new set of guidelines to help companies prepare for the GDPR, which will become enforceable in 25 May 2018. While addressed to small and medium companies, the documents can be used by organisations of any size, and are likely to constitute an important reference point in their interactions with a Data Protection Authority that is known for being active in the field of enforcement.

The guidelines focus on three key areas:

Guidelines for Data Controllers – focusing on the main topics for controllers to ensure compliance with the Regulation (with clarifications on aspects such as legal grounds, data subject rights and concrete examples of how the accountability principle and a risk-based approach may be implemented). The guidelines also contain a question-based checklist to guide controllers through these obligations and help them assess the level of compliance of their data processing operations.

Guidelines for Agreements between Data Controllers and Data Processors – providing an explanation on the contract or legal act that will be required to bind these two actors, and offering insights into the minimum content of this agreement.

Guidelines for Complying with the Duty to Inform – with recommendations and practical insights into making available the information required by the GDPR. The document offers an explanation of each requirement as well as examples of information notices.

These guidelines can be found in a dedicated new area of the official AEPD webpage, which also contains additional guidance on GDPR-related topics.

In the same press release, the AEPD also announced its intention to make available a self-assessment tool for organisations wishing to progressively adapt to the GDPR. The tool will allow organisations to assess the risk profile of their envisaged data processing operations and guide them towards recommended measures.

Australia introduces data breach notification procedure

Amending the Privacy Act of 1988, the Australian Senate has introduced a mandatory data breach notification scheme on 13 February 2017. Agencies and companies will, from a set moment in time communicated by the Federal Government, be obliged to notify data breaches to the Australian Data Protection Authority (i.e. Australian Information Commissioner). Additionally, the affected data subjects have to be informed about all data breaches that provide a high risk to the rights and freedom of the data subjects and are most likely to result in a serious harm for the data subjects affected.

All “APP” entities (agencies, individuals, commercial organisations, unincorporated associations, partnerships, trusts) that fall within the scope of the Privacy Act will have to comply with the new procedure. More specifically these entities cover all private sector and non-for-profit organisations having an annual turnover of more than three million Australian dollars (1), Australian and Norfolk Island Government agencies (2), private health service providers (3) a few small businesses (4) and number credit reporting bodies holding credit information (5). Furthermore, these entities need to handle, use and manage personal information and are expected to secure the personal data under the Privacy Act.

The amendment states that notification is triggered as from the moment the APP entity has a reasonable ground to believe that an eligible data breach has happened, or in case it is directed to do so by the Commissioner. A notice should be communicated using whichever method is commonly used to interact with the individual impacted by the breach and should include the following information: the company’s identity and contact details, a description of the eligible data breach that the company has reasonable grounds to believe has taken place, the type or types of information concerned, as well as recommendations about the steps that will be taken in response to the data breach.

Eligible data breaches happen when there is unauthorised access to, unauthorised disclosure of or loss of personal information held by an entity and the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates to. Companies suspecting that a data breach occurred, need to carry out an assessment of the situation within thirty days after becoming aware of the reasonable grounds to believe so.

Companies that fail to comply with the new data breach notification will be subject to investigations, enforcement and amongst others civil penalties up to $1.8 Million for serious breaches or repeating ones.

The new bill also states that in the event companies have taken remedial action in order to rectify an eligible or potential data breach and if data subjects could reasonably conclude that the breach would not lead to serious harm (as explained in the explanatory memorandum) to the affected data subjects, companies are exempted from the obligation to notify.

The Australian Information Commissioner has stated that the introduction of the mandatory breach notification scheme is welcomed as it will strengthen the data subject's privacy and increase transparency for the public on serious data breaches.

New Argentinian draft bill for a data protection act

In February 2017, the Argentinian Data Protection Authority has issued a draft version for a new data protection bill. The new act will repeal the current data protection act of 2000. Since Argentina was one of the first countries considered adequate by the European Union, it is important to pinpoint that change has been instigated against the background of the General Data Protection Regulation, applicable as from 25 May 2018. The draft bill will be open for public consultation until 24 of February 2017.

The bill would overhaul the current section relating to international data transfers and introduce new principles including amongst others: the abolishment of the obligation to register databases (1), the sole acknowledgement of individuals as data subjects (no longer legal entities) (2), the introduction of new definitions such as for biometric and genetic data (3), the addition of legal bases for processing personal data next to consent (4), the principle of privacy by design (5), the obligation to carry out privacy impact assessments (6), the obligation to appoint Data Protection Officers (7), and others.

Furthermore the draft bill amends certain provisions with regards to credit reports, including the time limit to keep negative data and the obligation to notify an individual in the course of an agreement not concluded due to negative information included in the credit report. While the draft bill applies to data subjects, it no longer applies to legal entities. As a consequence, financial information of companies would no longer be in scope.

Lastly, the draft bill confirms the independence of the Argentinian Data Protection Agency as being separate from any other governmental institution and thereby remedies an observation made earlier by the European Union at the time where Argentina was recognised as an adequate country on the level of data protection.

It is expected that the new law will be sent over to the Argentinian President by the end of 2017 and will be discussed in Congress at some point during 2018.

WP29 finalises guidance on DPO, data portability, lead authority, and proposes guidance on DPIA

During early April 2017, the Article 29 Working Party ("WP29") produced several pieces of important guidance surrounding the impact and implementation of the General Data Protection Regulation ("GDPR"). After review of the comments received during the public consultation rounds, the WP29 published its final guidance on data protection officers ("DPO"), lead authorities and the right to data portability. In addition, the Working Party published its draft guidance on data protection impact assessments ("DPIA"), which is now open to public consultation.

Overall, no major changes have been made to the earlier draft guidance on these three topics. That being said, WP29 has provided useful clarifications that organisations should take into account when preparing for compliance.

The guidance, amongst others, suggests that a DPO should be located within the European Union in order to be accessible. Confirming that only one single person can be designated as DPO, it has now become clear that this person may in fact be supported by a team. Interestingly, both the DPO and/or members of its supporting team can be engaged on the basis of a service contract. Another notable clarification concerns the conflicts of interest of internally appointed DPOs; as a rule of thumb, senior management positions as well as lower positions (if they determine the purposes and or means of processing) may qualify as conflicting and could therefore not be eligible for a role as DPO. Hence, it is recommended that organisations seeking to appoint an internal DPO carefully evaluate the potential candidates' position, tasks and job description for any indications of conflict of interest. In addition, WP29 stipulates that the DPO's obligation of secrecy does not prohibit it from contacting and seeking advice from supervisory authorities.

On the right to data portability, clarifications provided by WP29 include the notion that controllers should implement specific procedures with its data processors in order to adequately handle data portability requests. Ensuring the effectiveness of such measures requires diligent cooperation of both parties, which is best captured in adequate contractual provisions and obligations. The guidance also clarifies that any personal data processed out of the scope of the legal grounds of consent or performance of contract, such as personal data processed by a financial institution as part of its anti-money laundering obligations, is out of scope of data portability. Further specification concerns the types of data that should be made portable: personal data observed from the activities of users now also includes activity gathered by connected objects other than smart meters, activity logs and histories of website usage or search activities. Inclusion of 'observed' personal data in the scope of the right to data portability has faced criticism as an undue enlargement of its scope. As such, data does not strictly equate as personal data 'provided by' the data subject.

Final guidelines on determining lead supervisory authorities, as part of the GDPR's one-stop shop mechanism, clarify that joint controllers should define amongst themselves whose establishment will serve to determine the lead supervisory authority. Most notably, where the draft version of this guidance included an example indicating that an organisation would have to report data breaches to its lead supervisory authority, this example has been deleted. While this does create some uncertainty, this also suggests that WP29's future guidance on data breach reporting will include guidelines in this respect.

In its draft DPIA guidance, WP29 provides useful insight into the criteria that determine whether performing a DPIA is mandatory, as well as key takeaways regarding the use of existing methodologies to carry out a DPIA. Interestingly, the draft guidance also

includes WP29's criteria for an acceptable DPIA, which further strengthens the notion that organisations are allowed some flexibility in tailoring a DPIA process provided that a certain quality threshold is met. Organisations that already perform these assessments are recommended to evaluate whether their approach meets the WP29 criteria.

Recent breaches and enforcement actions

Court Rules against Forced Fingerprinting

A federal judge in Chicago has ruled against a government request that would force a citizen to "provide his fingerprints onto the Touch ID sensor of any Apple iPhone, iPad or other Apple brand device in order to gain access to the contents of any such device". "The government", Judge M. David Weisman wrote, "could seize such devices but not compel individuals to provide their fingerprints". You can find the ruling here.

While lack of probable cause seems to have been the deciding factor, the Judge (a former federal prosecutor and former FBI special agent) also cited concerns over the legality of such a measure under the Fourth Amendment, which grants rights to residents in the context of search and seizure, and the Fifth Amendment, which protects against self-incrimination.

While not legally binding, the ruling does set a precedent. It is the latest judicial development in a series of cases that have pitted US government agencies and bodies against password protected and encrypted devices in the context of security and crime fighting.

Earlier this year in January, a Minnesota appellate court ruled against a convicted burglar who was forced to unlock his phone with his fingerprint (State of Minnesota v. Matthew Vaughn Diamond). In this case, providing a password or fingerprint was considered akin to relinquishing a key to a locked vault, rather than an act of self-incrimination. Similarly, a Virginia Court judge ruled in 2014 that while police officers cannot force criminal suspects to divulge cell phone passwords, they could force them to unlock a phone with a fingerprint scanner.

The topic is also related to recent concerns over the ramp up in electronic media searches at the US border. According to the US Government, the number of searches has increased from 4 764 occurrences in 2015 to 23 877 in 2016, and authorities may demand the password to access a device as a pre-condition to be admitted entry into US territory. As non-US citizens are more vulnerable to intrusions on their privacy or personal property, travellers to this country should consider beforehand whether they can reduce the amount of information that they carry across the border (for example, by not carrying certain devices, using temporary devices, or deleting content).

Not a right to be forgotten in Public Companies Registry, but a right to object

Salvatore Manni, an Italian company director brought an action against the Lecce Chamber of Commerce requesting the removal of his personal data from the Public Registry of Companies. Mr. Manni's complaint was based on the ground that he was losing clients due to the appearance in the public registry of the liquidation of a company under his administration more than 10 years before. The court proceedings led the Italian Court of Cassation to refer several questions to the CJEU for a preliminary ruling, including whether the Directive 95/46/EC on data protection (DPD) and the Directive 68/151 on disclosure of company documents preclude any person from accessing data relating to natural persons set out in the companies registry without any time limits.

The CJEU held that the DPD was applicable and after recalling that these provisions must be interpreted in the light of the fundamental rights guaranteed by the Charter and especially Articles 7 and 8, the CJEU found that the processing activities of the public register were based on the grounds of compliance with a legal obligation and the realisation of a legitimate interest pursued by the controller or by the third parties to whom the data are disclosed. The CJEU furthermore stated that "in the event of failure to comply with the condition laid down in Article 6(1)(e) (data retention), Member States guarantee the person concerned, pursuant to Article 12(b) thereof, the right to obtain from the controller, as appropriate, the erasure or blocking of the data concerned". Furthermore the Court held that data subjects should be granted the right "inter alia in the cases referred to in Article 7(e) and (f) of that directive, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation".

In its assessment on the right to erasure and to object, the CJEU took into account the purposes of the processing operation, which in this case was "to protect in particular the interests of third parties in relation to joint stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets" and "to guarantee legal certainty in relation to dealings between companies and third parties in view of the intensification of trade between Member States". In view of the above, the CJEU held that even if there is no dedicated provision in Directive 68/151 " it is common ground that even after the dissolution of a company, rights and legal relations relating to it continue to exist and questions requiring such data may arise for many years after a company has ceased to exist", without however being able to "identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary".

The CJEU took into consideration the "limited number of personal data items" required by Directive 68/151 and that "it appears justified that natural persons who choose to participate in trade through such a company are required to disclose the data relating to their identity and functions within that company, especially since they are aware of that requirement when they decide to engage in such activity". **Therefore, the CJEU held that the data retention principle and the right to erasure provided by the DPD do not guarantee the right to obtain "as a matter of principle, after a certain period of time from the dissolution of the company concerned, the erasure of personal data" under those particular circumstances.**

Nevertheless, the CJEU noted that "it cannot be excluded, however, that there may be specific situations in which the overriding and legitimate reasons relating to the specific case of the person concerned justify exceptionally that access to personal data entered in the register is limited, upon expiry of a sufficiently long period after the dissolution of the company in question, to third parties who can demonstrate a specific interest in their consultation"

In conclusion, the CJEU reinstated that it is incumbent to national courts and on a case by case basis consideration to undertake the balancing exercise between the interests of third parties to have access to data published in the Companies Registry and the rights of the individuals to obtain erasure of the data and to object to its processing. However, in the case of Mr. Manni the CJEU estimated that "the mere fact that, allegedly, the properties of a tourist complex built … do not sell because of the fact that potential purchasers of those properties have access to that data in the company register, cannot be regarded as constituting such a reason, in particular in view of the legitimate interest of those purchasers in having that information".

Privacy events around the globe

European Privacy Academy

Dolce La Hulpe, Belgium
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:

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

IAPP Asia Privacy Forum

Singapore, 24 – 25 July 2017
https://iapp.org/conference/iapp-asia-privacy-forum/

The International Association of Privacy Professionals (IAPP)'s Asia Privacy Forum returns to Singapore, bringing high-end discussion and education on current trends and challenges in the Asia-Pacific privacy landscape as well as the rest of the globe. This year's edition will also include a pre-conference workshop with a focus on practical GDPR compliance.

Privacy. Security. Risk 2017

San Diego, California, 16 – 18 October 2017
https://iapp.org/conference/privacy-security-risk/

2017's P.S.R. brings its intensive cross-industry program to the west coast's San Diego, California. With an opening session planned for Monday October 16, followed by a two day conference on Tuesday 17 and Wednesday 18 October, plenty of brand new security, IT, and privacy offerings will be included, as well as GDPR preparation and education break-outs.

IAPP Europe Data Protection Congress 2017

Brussels, Belgium, 7 – 9 November 2017
https://iapp.org/conference/iapp-europe-data-protection-congress/

True to its three day format consisting of workshops and conferences, the IAPP Europe Data Protection Congress offers an unparalleled forum for lively debate, interaction, and exchange between regulators, data protection experts and privacy professionals from Europe (and beyond).

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
Partner
Cyber Risk Services