Deloitte.

Belgium | Audit & Enterprise Risk Services | February 2015

Privacy Flash
Belgium

Privacy at your fingertips

Privacy is becoming increasingly important to everyday business. Legal developments happening in the area and regulators' increasing attention on privacy are two of the key driving motives for that.
The aim of the "Privacy Flash" series is to bring to an audience eager to learning more about privacy, selected information on regulation, awareness events and initiatives related to personal data protection, as well as indicative privacy-related topics and projects the market seems to be busy on.

We hope that you will find this bi-monthly news series interesting. For additional information or suggestions on how to improve the "Privacy Flash", please contact Georgia Skouma.

Issue 3
February 2015

EU Data Protection Reform

News

At the 9th European Data Protection Day, Vice-President Ansip and Commissioner Jourovà made a joint-statement on the importance to conclude the EU Data Protection Reform, which is one of the top priorities for 2015 of the EU Commission. The goal is to conclude the ongoing negotiations on the data protection reform before the 28th of January 2016 (10th European Data Protection Day).

Currently, the proposal Data Protection Regulation is under Council's review in view of reaching a common position on the amendments to be made. Once the Council has agreed on a common position, next step would be the start of the "trialogue" discussions between the Parliament, the Commission and the Council.

So far, the Council managed to reach a "partial general agreement" on main points such as international data transfers and the approach to controller's and processor's obligations. In addition, Member States have agreed on the approach to "the one-stop shop" but not yet on the full details of the scheme. More information on the Council negotiations is available on the Information Commissioner's Office blog.

In a nutshell, the Council seems to be in favor of a risk-based approach, which implies more flexibility and greater freedom for Member States compared to the initial proposal such as amended by the Parliament. According to the Council, obligations such as Privacy Impact Assessments (PIA), prior consultation with the DPAs, as well as data breach notification should apply only in case of "high-risk" processing activities or to organizations with more than 250 employees.

At the CPDP conference in Brussels on 22 January 2015, Jan Albrecht, MEP and data protection rapporteur at the European Parliament on the draft EU Data Protection Regulation, shared his optimism about the Council reaching a common position by the end of summer 2015 and hence, the likelihood that the Data Protection Regulation is adopted by the end of this year. Nevertheless, it is important to note that even if this is the case, the Regulation will not be enforced before 2017.

For more information on the changes that will be introduced by the new Regulation, please refer to our previous Privacy Flashes.

Data localization Law in Russia

Different enforcement date?

The new Data Localization Law No. 242-FZ which would require personal data of Russian citizens to be stored and processed in databases located in Russia will enter into force earlier than foreseen. Originally, the law was expected to be enforced on 1 September 2016 but after the amendments that took place in December 2014, the law will now enter into force one year earlier, on 1 September 2015. More information on the Data Localization Law is available on our website.

On 17 December 2014, the Duma (lower chamber of the Parliament) voted in favour of the Federal Law No. 526-FZ amending the effective date of the Data Localization Law No. 242 – FZ to 1 September 2015. The new law was approved by the Federation Council on 25 December 2014 and signed by the President on 31 December 2014, meaning that it is now formally adopted. Please click here for more information.

Earlier enforcement of the law will increase the risks of non-compliance as it leaves organizations with limited time to adapt to the changes introduced by the new law. The uncertainties related to the interpretation of certain provisions of the law make it even more difficult for organizations to prepare properly for effective implementation. This being said, it is expected that a subordinated legislation is adopted before the enforcement of the law which will clarify how the law should be interpreted.

Right to be forgotten

Google will remove only EU search results

The Guidelines adopted by the Article 29 Data Protection Working Party on the implementation of the EUCJ judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (C-131/12) raised a number of hot topics. One of them relates to the territorial effect of the de-listing that search engine operators, such as Google, are obliged to effectively ensure after an individual requests deletion of his data and his request is found to be valid. Concretely, the Guidelines state that *"In practice, (…) in any case de-listing should also be effective on all relevant domains, including .com.".* Such an interpretation extends the territorial effect of the right to be forgotten outside of the boundaries of the European Union, territory over which the EUCJ has primarily jurisdictional competence.

Contrary to the Guidelines, Google expressed its intent to apply de-listing requests only at EU level. In other words, Google would only remove relevant search results from EU websites such as Google.fr or Google.be but not from the Google.com domain.

Click here for the full text of the guidelines.

For more information on the case and the guidelines, please refer to our previous Privacy Flash issues.

New Data Protection Law in Chile

Based on the EU Data Protection Directive

Chile is preparing a new privacy law based on widely acknowledged European and international data protection standards. The preliminary draft reflects the experience in privacy data protection in Chile and is shaped as to incorporate the standards in a number of privacy data protection instruments such as:

- Resolution of Madrid
- EU Data Protection Directive 45/96
- Proposal EU Regulation on Data Protection
- OECD Guidelines on the protection of privacy and trans border flows of personal data
- Law 15/1999 of Spain on Data Protection
- Law 8968 of Costa Rica on Data Protection

The new privacy law would create a Data Protection Authority and would increase the maximum fine.

The draft was subject to public consultations in July - August 2014. Although the text has not yet been published, you may be able to find more information on the website of the Ministry of Economy, Develiopment and Tourism of Chile.

US Cybersecurity Proposal Legislation

Legal immunity for companies sharing cyber threat information & strengthened enforcement

In 2014, the US Congress passed a cybersecurity legislation focused on improving the organization of cybersecurity missions. The legislation includes a number of bills: the Federal Information Security Modernization Act of 2014, the National Cybersecurity Protection Act of 2014, the Cybersecurity Enhancement Act of 2014 and the Cybersecurity Workforce Assessment Act of 2014.

Following the Sony Pictures hack attack, the Congress updated the legislative proposal as to enable the sharing of cybersecurity information between the private and the governmental sector. Highlighting the importance of cybersecurity, President Barak Obama announced the proposed legislation on 13 January 2015.

The proposed legislation would encourage companies to share hacker threat data with governmental agencies including NASA. Companies sharing such data will be covered with immunity from lawsuits. In addition, the proposal contains provisions that would allow for the prosecution of the sale of botnets; would criminalize the overseas sale of stolen U.S. financial information like credit card and bank account numbers; would expand federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft and would give courts the authority to shut down botnets engaged in distributed denial of service attacks and other criminal activity.

The purpose of this new legislation would be to facilitate the sharing of real-time appropriate cyber threat information with the National Cybersecurity and Communications Integration Center (department of Homeland Security) and to strengthen enforcement measures. Yet, privacy groups raised their concerns about whether this additional legislation is really needed, arguing that existing laws allow companies to coordinate sufficiently with the federal and state investigative, law enforcement and secret services in the prevention and combatting of cyber threats and cyber-attacks.

The White House blog provides more information on the topic.

Surveillance of Electronic Communications for Intelligence and National Security Purposes

WP29 Follow-up after Snowden revelations

On 5 December 2014, the WP29 released a Working Document on the Surveillance of Electronic Communications for Intelligence and National Security Purposes. This Working Document comes as a follow-up of the previously adopted *Opinion on surveillance of electronic communications for intelligence and national security purposes* issued on 10 April 2014, in the context of the Snowden revelations.

The document contains the legal analysis behind the Opinion of 2014 and provides recommendations on how to restore respect for the fundamental rights of privacy and data protection by the intelligence and security services.

The key points made by the WP29 in the working document relate to the interpretation of “national security” and to the applicability of the “national security exemption”.

The Treaty of the European Union (TEU) foresees an exemption of the applicability of the EU legislation for national security matters (art. 4(2)). However, in order to determine when this exemption may apply it is necessary define what the scope of “national security” is.

In the absence of a definition of “national security”, the WP29 suggests that in order to assess whether or not something should be defined as falling under the scope of “national security”, it is necessary to take into account the political situation at the time the “choice” is made as well as the relevant actors. Furthermore, the WP29 clarifies that if activities by intelligence and security services are generally considered as falling under “national security”, this is not always the case when general law enforcement authorities fulfill similar tasks.

The “national security exemption” such as foreseen in the TEU relates to EU Member States which leads to the question on whether such exemption exists for third countries. On that point, the WP29 clearly states that the exemption in the treaties offers no possibility to invoke national security of a third country in order to avoid the applicability of EU law.

Privacy at the Work Place

Opinion and Recommendations of the Belgian Privacy Commission

At the International Data Protection Day of 28 January 2015, the Belgian Privacy Commission decided to dedicate specific attention to the protection of the private life of employees at their working place. In this context, the Privacy Commission provided useful information on its website, as well as guidelines on the protection of private life for employees and employers. This information is available both in Dutch and in French. Various related topics are discussed and presented on the Privacy Commission website such as the control of alcohol and drugs consumption at work, camera surveillance, the usage of badge systems, geographical localization, biometric systems, social media.

The Privacy Commission issued as well an opinion and a consolidated version of existing recommendations on the privacy protection at work. The document is entitled “*Private life at work: myth or reality*?”, but is only accessible in French and in Dutch.

Recent breaches and enforcement actions

News on data breaches appearing in the press during last month

A health insurance company was the target of “very sophisticated” cyberattack. Personal data of company’s associates and customers were accessed during the data breach. For more information, please visit: http://www.anthemfacts.com/

Enforcement cases

In December 2014, the German DPA of Rhineland-Palatinate has imposed a fine of 1.3 million euros to an insurance company for violation of data protection laws and lack of internal controls. More information is available on their website.

In January of this year, Google Inc has committed to the UK ICO to make further changes to its Privacy Policy.

Deloitte & Privacy recent “wins”

Highlighted below are some of the projects our team of security specialists and lawyers assisted clients with during the last two months:

- Conduct of a Privacy Quick Scan for the Belgian offices of a worldwide, leading humanitarian organization.
- Assist a multinational hotel chain with headquarters in Spain and properties in Europe in the design of adequate mechanisms to cover cross-border data flows.
- Kick off a multidisciplinary study conducted by European Commission DG TAXUD on the evaluation of several policy and legal scenarios with a view to the implementation of a Tax Identification Number (TIN) in Europe.

- Assist a leading clothing manufacturer based in the US in the privacy assessment of an employee reporting line (whistleblowing) in a number of European and non-European affiliates and the submission of registrations to the National Data Protection Authorities (DPA) when needed.
- Advise a multinational biotechnology company based in the US with many affiliates in Europe in the design of customer privacy notices and harmonized opt-ins.
- Advise several companies from all industry sectors on several aspects of the adoption of the draft Data Protection Regulation and the current regulatory trends related to employee work time monitoring.

Past & forthcoming interesting events

8th International Conference CPDP

The 8th edition of the international conference Computers, Privacy and Data Protection (CPDP) 2015 took place in Brussels, Belgium on the 21 – 23 January 2015. The 3 days conference offered 70 panels, workshops and special sessions with 415 speakers from academia, public and private sectors and civil society.

Deloitte was actively involved with two panels on the topics of cyber-resilience and cybersecurity governance and a Wifi Hacking Demo to raise awareness of what internet users can do better to protect themselves against malicious use of their personal data.

For more information on the conference, please visit http://www.cpdpconferences.org.

Regional Conference Privacy in Digital Age

A regional Conference on Privacy in Digital Age was held in Prishtina, Kosovo (26 - 28 January 2015) with the active contribution of many neighboring national Data Protection Authorities, Kosovar academia and local business. The conference was organized in the context of the campaign launched by the National Agency for Protection of Personal Data in Kosovo in view

of increasing awareness of citizens about their privacy rights. The local Data Protection Authorities of the Balkan region shared their experiences over the applicability and enforcement of their local data protection laws, taking stock of the “lessons learnt” from other countries and regions, such as Europe and Japan.

For more information on the conference, please visit http://www.pda-ks.com

Upcoming events

Global Privacy Summit 2015

Washington, DC, 4 – 6 March 2015
https://privacyassociation.org/

IAPP Europe Data Protection Intensive 2015

London, 14 – 16 April 2015.
https://privacyassociation.org/

European Privacy Academy – Data Protection Officer Course

La Hulpe, European Privacy Academy,
Follow-up session on 28 April 2015
Visit our Deloitte website for more information.

Berkenlaan 8A, 8B, 8C
1831 Diegem
Belgium