Deloitte.

Belgium | Audit & Enterprise Risk Services | May 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 4
May 2015

EU Data Protection Reform

News

The Council of the EU announced on the 13th of March that it has reached a partial agreement with regard to the one-stop-shop principle, which aims at simplifying logistics for businesses and reducing any chance of multiple and possibly inconsistent requirements from different national Data Protection Authorities within the EU. According to the Council of the EU, the one-stop-shop principle will only be applicable in important cross-border cases where international cooperation is vital. The competent lead authority can be determined on the basis of (i) the main establishment of the controller; (ii) the main establishment of the processor; (iii) the Member State where the complaint was lodged. The lead supervisory authority will act more as a coordinator between the other concerned national authorities in Member States, where the controller or processor has an establishment, rather than a sole decision maker. Furthermore, in cases where the lead authority fails to reach an agreement with the other interested national authorities, the decision must be referred to the European Data Protection Board.

By way of exception, the rules regarding the lead supervisory authority and the one-stop-shop mechanism will not apply where the processing of personal data is carried out by public authorities or private bodies acting in the public interest. In such cases, the public authority or private body established in the relevant EU Member State will be the sole competent body.
It must be highlighted though that, as the Council has repeated consistently, nothing is agreed until everything is agreed. You may wish to read the official press release and the Presidency document with regard to the one-stop-shop mechanism.

Cyber Crime

Council of EU starts discussions on NIS Directive

The Latvian presidency of the Council of the EU announced in the beginning of March that is ready to resume informal trilogue meetings attended by representatives of the European Parliament, the Council and the European Commission, with the purpose to reach an agreement on a Draft Directive on Network and Information Security, the so-called NIS Directive).

According to this proposal:

- EU Member States will have to put in place a minimum level of national capabilities by establishing NIS national competent authorities, setting up well-functioning Computer Emergency Response Teams (CERTs) and adopting national NIS strategies and national NIS cooperation plans;

- NIS national competent authorities will have to exchange information and cooperate in order to counter NIS threats and incidents;
- Operators of critical infrastructure (e.g. energy, transport, banking, stock exchange, healthcare), key internet enablers and public administrations will be required to assess the risks they face and to adopt appropriate and proportionate measures to ensure NIS. These entities will also be required to report to competent authorities, any incidents with a significant impact on core services provided.

All documents relevant to the European Commission's proposal with regard to the "NIS Directive" are available from the EC Digital Agenda for Europe webpage.

Data Retention

European Commission confirms there will be no new Data Retention Directive

The European Commission has confirmed in a recent press conference that it does not intend to prepare a new Data Retention Directive further to the annulment of Directive 2006/24/EC by the Court of Justice of the European Union on 8 April 2014.

The annulled Data Retention Directive pertained to the processing of personal data with regard to publicly available electronic communications services or public communications networks and would amend Directive 2002/58/EC as a response to terrorist attacks in London and Madrid. In particular, the Data Retention Directive required telecommunications providers to retain traffic, subscriber and location data generated by users of their service for the purposes of investigation, detection and prosecution of serious crime and terrorism.

As a reminder: On the grounds of the Court's judgment "by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interfere[d] in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data". According to the Court, the Directive was not proportionate with regard to the purpose it was meant to achieve, i.e. the prevention of crime, and interfered seriously with the rights to privacy and personal data protection of individuals guaranteed by the Charter of Fundamental Rights.

Privacy at the workplace

Council of Europe's Recommendation on the processing of personal data of employees and job candidates

On 1 April 2015, the Council of Europe issued a Recommendation on the processing of personal data in the context of employment. This document, which replaces Recommendation (89)2 formerly published on the same subject, sets out the principles that governments of Member States are recommended to reflect in the application of domestic legislation on data protection in the employment sector as well as in other fields of law involving personal data processing in the context of employment.

While the document reiterates the basic principles for lawful processing of personal data laid down in the Data Protection Directive currently in force, it also refers to contemporary issues and practices, such as the use of social media, equipment revealing the employees' location, whistleblowing and psychological tests. For instance, as per the Council's recommendation employers should fully inform or consult with their employees prior to introducing measures designed to monitor their movements or productivity. Furthermore, the performance of tests or analyses to assess the character or personality of employees and job candidates should not take place without their prior consent or other appropriate safeguards provided for by the national legislation.

Cloud computing

Amazon cloud contract terms are found to meet EU standards on data transfers by Luxembourgish DPA

The National Commission for Data Protection in Luxembourg (CNPD) stated that contract terms employed by the cloud provider Amazon Web Services (AWS) "make sufficient contractual commitments to provide a legal framework to its international data flows" which are in line with the relevant EU data protection rules with regard to international data transfers. The CNPD's official announcement is available on their website.

It must be noted that CNPD was acting on behalf of Article 29 Working Party, which issued a similar endorsement last year regarding Microsoft. According to this decision, the Amazon clauses should not be considered as "ad hoc" clauses but rather as Standard Contractual Clauses as approved by EU Commission by means of Decision 2010/87/EU. The CNPD considers that this approval will result in the reduction of the numerous authorisations required by national Data Protection Authorities within the European Union for the transfer of personal

data to third countries when companies conclude a contract with AWS involving storage of personal data.

Privacy Enforcement

Damage Actions in the UK

In a recent case (Google Inc. v Vidal-Hall and Others) the UK Court of Appeal has ruled that there is a tort of “misuse of private information” and any company which is found to have violated privacy rules is liable to pay damages to individuals irrespective of whether they have proved to have suffered harm or not.

The judgement may have severe financial and reputational implications not only for Google but for any other company found in breach of privacy rules as they can be subject to a large amount of individual damage claims. It is noteworthy however, that the Court also stated that any damages awarded to claimants in such cases will be “relatively modest”. The full text of the judgment is available here.

Deloitte & Privacy recent “wins”

Highlighted below are some of the recent projects our team of privacy and security specialists have been assisting clients with:

- Assist the European Union Agency on Network and Information Security (ENISA), to collect and validate information on the means and approaches European countries are currently using for exchanging information about cyber incidents.
- As member of a consortium, conduct a multidisciplinary study on the design of an EU-wide cooperation platform to enhance the interconnectivity and cooperation of the Computer Emergency and Response Teams of the European Union. The aim of the platform is to strengthen European preparedness and response to emerging cyber threats.

- Support an international payment service provider with an international presence in reviewing its privacy program, and more specifically its international data transfer aspects with a view to ensuring the program's compliance with international and European good practices in personal data protection.
- Assist an international car manufacturer in implementing a multidisciplinary set of activities aiming at strengthening the company's compliance with European data protection rules and practices.
- Quick scanning of an email filtering solution that one of our clients (active in the financial sector) envisages to roll out in many countries in Europe to prevent data leakage.
- Help a well-known leader of the financial services sector to understand the key requirements and restrictions related to data monitoring.
- Advise several companies from all industry sectors on several aspects of the adoption of the draft Data Protection Regulation.

Past & forthcoming interesting events

Annual Conference on European Data Protection Law

Brussels 11-12 May 2015
https://www.era.int/

Organised by the Academy of European Law with the support of the European Data Protection Supervisor (EDPS), the conference provided practitioners with a comprehensive update on recent developments in European data protection law. Amongst the topics discussed figured updates on the Draft General Data Protection Regulation and the negotiations over TTIP, the EU-US data protection "umbrella agreement", as well as some business-oriented presentations on the citizen's right of access to their data and the approaches business opt for today for achieving compliance with personal data protection rules.

European Privacy Academy - DPO Courses

La Hulpe, Deloitte University
Visit our website for more information

Courses will take place at the following dates:

- 5 – 8 May 2015 with a follow-up session on 8 September 2015
- 27 – 30 October 2015 with a follow-up session on 22 January 2016
- 18 – 21 January 2016 with a follow-up session on 15 April 2016

Homepage

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