Deloitte.

Belgium | Audit & Enterprise Risk Services | 31 October 2014

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 towards privacy are two of its key driving motives.
The aim of the "Privacy Flash" series is to inform an audience that is eager to learn more, about the latest news on 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 with.

We hope that you will find this bi-monthly news series interesting. For additional information or suggestions on

Issue 1
October 2014

how to improve the “Privacy Flash”, please contact Georgia Skouma.

“Right to be forgotten”: from letter to practice

Following the “Google vs. AEPD” ruling of the European Union Count of Justice (CJEU) on May 13, 2014, which resulted in the right to be forgotten, the Article 29 Working Party (the “Working Party”) announced on September 18, its decision to establish a common approach referred to as the “tool-box”. The background to this stance of the Working Party stems from the obligation of the search engines, as data controllers, to respect the CJEU ruling and to acknowledge the right of data subjects to be “de-listed”. However, the Working Party reports that the European Data Protection Authorities (DPAs) received numerous complaints resulting from search engines’ refusal to “de-list” complainants from their results, which demonstrates a genuine demand for data protection from data subjects.

As part of the “tool-box,” the Working Party intends to put in place a network of dedicated contact persons within the DPAs in order to develop common case-handling criteria for the complaints relating to the right to be forgotten. This network shall provide the DPAs with (1) a common record of decisions regarding the right to be forgotten, and (2) a dashboard to be used to identify the different types of complaints and highlight similarities.

As the development of the “tool-box” goes on, the Working Party has also announced that it will continue to analyse how search engines comply with the ruling. During the summer months, it also pursued its consultation process with stakeholders, such as media companies. Furthermore, following the CJEU May ruling, the Working Party prepared a common list of requirements and possible measures that Google could implement in order to guide the company in the implementation of the legal requirements regarding data protection. The guidelines have been elaborated in the context of the specific coordinated EU investigation into Google’s privacy policy. Similarly, the Working Party may also consider issuing guidance on specific issues to the entire industry, at a later stage.

The European Commission has published a factsheet concerning the “myths” related to the right to be forgotten.

Russia enacts Data Localisation Requirement

The Russian data protection landscape has seen some important developments in the past couple of months with the signing of a new Law No. 242-FZ "On Amendments to Certain Laws of the Russian Federation in Order to Clarify the Procedure for Personal Data Processing in Information and Telecommunications Networks", which is expected to enter into force on September 1, 2016 (though, it cannot be excluded that earlier effective date will be approved). The main changes include the obligation of data operators to ensure while collecting personal data that recording, systemisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data is to be conducted in databases located on the territory of the Russian Federation. While data operators failing to comply with the new law risk having their websites blocked in Russia and being listed in the Register of Personal Data Rights Violations, Russian experts believe that it will still be possible to transfer personal data abroad.

The current version of the new Law applies to all companies carrying out business activities in Russia that involve processing of personal data of Russian citizens, regardless of whether they have a physical presence in Russia. In practice, this mean that any foreign social networking, online shopping and other types of websites that receive information about Russian citizens will be required to install servers in Russia, and store or process information about Russian citizens only by using servers located in Russia. Deloitte Belgium is following the developments of this new legislation closely in collaboration with its Russian local experts and will bkeep you abreast of the follow-up.

Cookie Sweep Day

A European coordinated action of on-line audits
The "Cookie Sweep Day" (15 to 19 September) entailed a coordinated online audit of the main websites targeting European consumers operating in Europe to verify compliance with the 2013 EU cookie recommendations. This was done in the initiative of the Article 29 Working Party, and it was open to any DPA to take part in it. The DPAs will share the results of their respective audits with a view to making a comparison among Member States and possibly harmonising their positions with regard to cookies compliance in Europe. Although the purpose of the online audit was not to conduct enforcement actions, the results may be used by each DPA to enforce compliance with the cookie provisions under national law, which has already been the case in some jurisdictions. In France, for instance, the CNIL has the power to conduct on-site and on-line inspections that can be followed by administrative sanctions.
What should companies do in advance of this enforcement action? Some basic steps to comply with the cookie requirements include:

- Audit your websites to find out what types of cookies (or other tracking devices) you use
- Analyse the purposes of the cookies
- Assess the level of intrusiveness of cookies and verify which cookies require prior consent
- Publish a clear, understandable and accessible cookie policy on your website
- Implement an adequate cookie consent mechanism

Global ICO survey finds 85% of mobile apps fail to provide basic privacy information

A survey of over 1,200 mobile apps by 26 privacy regulators from across the world has shown that a high number of apps are accessing large amounts of personal information without adequately explaining how people's information is being used.

The survey by the Global Privacy Enforcement Network (GPEN) examined the privacy information provided by 1,211 mobile apps. As a member of GPEN, the UK's Information Commissioner's Office examined 50 of the top apps released by UK developers.

More information is available on the website of ICO.

Article 29 WP publishes statement on personal data retention

On September 5th, the Article 29 Working Party (WP29) released its statement on the ruling of the Court of Justice of the European Union which invalidates the Data Retention Directive. In this judgment, the Court ruled that the EU Data Retention Directive is invalid because it interferes disproportionally with the European citizen's rights to privacy and data protection.

In its statement, the WP29 urges the Member States and the European Institutions to evaluate its consequences on national data retention laws and practices in the EU. In particular, it should be ensured that no bulk retention of all kinds of data are made and that instead, data are subject to appropriate differentiation, limitation of exception. In addition, access and use by national competent authorities should be limited to what is strictly necessary and subject to substantive and procedural conditions, and national laws should provide effective protection for citizens. Finally, the WP29 urged the European Commission to provide further clarification and guidance on the consequences of the judgement.

More information can be found on the website of the European Commission.

The Internet of Things: EU regulators' opinion on its main privacy related risks

The concept of the Internet of Things (IoT), as stated by the Article 29 Working Party, refers to an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects to individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.

On September 22, 2014, the Working Party released an Opinion on IoT (the "Opinion"), intended to draw the attention to the privacy and data protection challenges raised by the IoT and to propose recommendations for the stakeholders to comply with the current EU data protection legal framework.

Specifically, the Working Party addresses (1) "wearable computing" such as glasses and clothes that contain computers or sensors, (2) "quantified self" such as fitness devices carried by individuals who want to record information about their own habits and lifestyles and (3) "domotics" which are devices in the home that can be connected to the Internet such as smart appliances. These are three important recent developments related to the IoT and considered by the Working Party to exemplify the current Internet of Things.

According to the Working Party, the main privacy, data protection and security issues that are currently raised by the IoT are (1) the user's lack of control over his or her data and information asymmetry; (2) the quality of the user's consent; 3) the repurposing of original data processing; (4) intrusive profiling and behavioural analysis; (5) difficulties to ensure anonymity and (6) security risks. In light of this, the Working Party stresses the fact that the EU Data Protection Directive 95/46/EC on the protection of personal data and the e-Privacy Directive 2002/58/EC as amended in 2009 are fully applicable to the processing of personal data through different types of devices, applications and services used in the context of the IoT.

The Opinion outlines a number of practical recommendations aimed at various stakeholders involved in the development of the Internet of Things, including device manufacturers, application developers, social platforms, further data recipients, data platforms and standardization bodies. The recommendations are intended to assist with compliance with most of the obligations provided by the EU data protection legal framework (e.g., consent requirements, legal bases for processing personal data, data quality and data security, specific requirements for processing sensitive data, transparency requirements, the rights of the data subjects).

Deloitte & Privacy recent “wins”

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

- Advice to companies of the leisure and hospitality sector and food manufacturing on design of cross-order data flows by implementing Binding Corporate Rules and Standard Contractual Clauses.
- Help a leading automotive supplier in the review of its privacy program & design of remediation actions
- On-going advice to companies to understand notice requirements related to the installation of cookies on their websites and the transposition of “opt in” requirements in local jurisdictions
- Advice to a biotech company on worldwide best practices regarding password lengths used in mobile devices.

Past & forthcoming interesting events

UIA conference on Personal Data Protection in the CJEU

http://www.uianet.org

The European Court of Justice (ECJ) opens its doors very rarely. However, this prestigious institution reacted positively to the suggestion of the Privacy & Human Rights Commission of the International Union of Lawyers (Union Internationale des Avocats - UIA) to organize a

seminar on data protection in the court's premises. Taking stock of the recent ECJ case-law relating to personal data retention (April 8, 2014) and the right to be forgotten (May 13, 2014), the seminar focused on the upcoming data protection legal reform, including the practical impact of the recent court rulings stated above. Besides the views of the European Commission and the national regulatory authorities on how the current legislative framework will evolve, participants of renowned multinationals, such as Google and Microsoft, as well as privacy counsels, amongst other Deloitte, gave their own perspectives on the reform and practical guidance on where private companies should focus compliance efforts.

Deloitte Privacy Academy Belgium

http://www2.deloitte.com/be/en/pages/risk/solutions/european-privacy-academy.html

The first courses of the European Privacy Academy were held. In September there was a department-specific course for HR professionals and on October 13th privacy professionals from different national and international firms gathered on the European Privacy Academy's campus for the first four days of the Data Protection Officer course. The fifth session of this course will be held on January 13, 2015.

Upcoming events

The IAAP Europe Data Protection Congress

Brussels, 18-20 November 2014.
https://privacyassociation.org/conference/iapp-europe-data-protection-congress-2014

Computers, Privacy & Data Protection Conference

Brussels, 21 – 23 January 2015.
http://www.cpdpconferences.org/

European Privacy Academy – Data Protection Officer Course

La Hulpe European Privacy Academy, 26 – 29 January 2015, with a follow-up session on 28 April 2015

Visit our Deloitte website for more information.

Homepage

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