Deloitte.

Belgium | Audit & Enterprise Risk Services | 22 December 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 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 2
December 2014

EU Data Protection Reform

News

The Presidency, the Commission and the Member States conducted a public session to provide updates on to the EU Data Protection Reform (recording available here: Justice and Home Affairs Council - Public session - 10 October 2014. The main message from this session, is that “nothing is agreed until everything is agreed”. In practice, this means that additional changes to the Regulation’s published draft might still occur in order to ensure the overall coherence of the new Regulation and probably less rigorous implementation objectives than the ones initially introduced. For example, Privacy Impact Assessments (PIA) may at the end become mandatory only for “high-risk” data processing operations. In the same vein, it seems that the Council is more inclined to leave some liberty to the Member States in defining key requirements with regards to the appointment of a Data Protection Officer.

During the closing session of the IAPP Europe Data Protection Congress (IAPP Europe Data Protection Congress 2014, see below)), it was also mentioned that - although certain points, such as the right to be forgotten, need further discussion - there seems to be a consensus amongst the EU bodies on some other key concepts introduced by the draft Regulation (for instance: the “one-stop-shop regulator”).
As a reminder, according to this new institution, companies (in particular multinationals which currently have to deal with many local DPAs) will be able to dialogue only with one DPA once the Regulation is adopted, this DPA being the one of the country of their main establishment in Europe. In principle, it will be the “lead” DPA’s role to tackle the matter and to coordinate with the other local DPAs that may possibly be involved in order to reach a single decision (“co-decision model”). The European data Protection Board will be able to intervene in the event of disputes between the different DPAs concerned.
On this “one stop shop regulator” mechanism, the Council seems to be in favor of a “proximity system” that will also encompass the remedial phase. Practically, the system should also facilitate the rights of redress that data subjects are entitled to exercise in case of privacy violations, allowing them to contact their local DPA irrespective of the place of location of the data controller.

In terms of timing, the New European Commission has set as goal to finalize the negotiations in the course of 2015.

Data localization requirements in Russia

Updates

On 5 November 2014, the 5th International Conference on personal data protection was organized by the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Russian DPA – *Rozcomnadzor*) in Moscow.

As expected, the new data localization law (see "Russia enacts data localization requirement" published in Privacy Flash, Issue 1) was one of the core subject matter areas tackled at the Conference. During the conference, the Russian DPA reiterated that secondary legislation would be brought forward in the near future to help citizens and businesses to better understand the practical impact of the new restrictions and comply effectively with those.

Other points that have been clarified during the conference are:

1. The new restrictions will apply to all operators irrespective of industry sector.
2. Cross-border data transfers will still be allowed once the amendments come into effect, as Russia is still bound by Convention of the Council of Europe n°. 108 on the protection of personal data during automated data processing. Practically speaking, this implies that operations on the internet (e.g. hotel booking through a tour operator based outside of Russia) initiated by Russian citizens will still be possible.
3. If a foreign company (e.g. website operator) is located outside of Russia but its services actively target Russian citizens, it will be bound by the localization restrictions enounced in the new law. This practically means that foreign service providers will have to ensure that the personal data related to Russian citizens will be collected, stored and processed in the first instance in Russia.

Poland: Regulatory amendments soften *regime* on cross-border data transfers and notifications

On January 1st, 2015, important amendments to the Polish Personal Data Protection Act will enter into force. The amendments set out new rules of data transfer to non-EEA countries and the notification *regime* of data filing systems. The latter is also related to a new type of data protection officers to be appointed by the data controllers in Poland.

As from the new year and based on the Commission's standard clauses on cross-border data transfers, it will no longer be required to get the approval of the Polish Data Protection Authority (GIODO) each time that a data controller transfers personal data outside Poland. Secondly, starting January 1st, 2015 it will be possible to request GIODO for approval of binding corporate rules implemented in international corporations at international level. If Binding

Corporate Rules have already been approved by data protection authorities in another country, GIODO may issue the approval based on consultations with the lead authority.

Thirdly, according to the new law, the appointment of a *data protection officer* of a new type (DPO) will be voluntary. The appointment of the DPO will relieve the company from the obligation to register their personal data filing systems with GIODO. Note that the above exemption does not apply to sensitive data files which will still have to be notified to GIODO. The obligation to register will be transferred from GIODO to DPO, who will be responsible for internally maintaining a register of personal data filing systems.

For more specific information regarding these important changes please contact our legal correspondent Tomasz Rutkowski, managing associate in Deloitte Poland.

Right to be forgotten

Guidelines of European regulators on its effective implementation

Following the ruling of the Judgment on the Google Case [C-131/12], the Article 29 Data Protection Working Party has adopted a set of guidelines (the 'Guidelines') to clarify how the local Data Protection Authorities intend to implement the judgment.

On the question how to evaluate the legitimacy of data subjects' requests to have their data removed by search engines, the Working Party emphasized the need to strike the right balance between the economic interest of the search engine and the right of end users to have access to information. According to the Working Party, the judgment clearly draws an obligation of result, meaning that in practice a request of "de-listing" may not be restricted to the EU territory (in principle, being the expected scope of EU Court rulings) but could be extended to an obligation of removing information from all internet domains, including the ".com" ones. An important clarification given in the guidance is that the right of de-listing applies only to the results obtained if performing a search using the name of the individual. Thus, the right does not imply the complete deletion of the page from the indexes of the search engine, which should remain accessible if one uses other search terms or criteria.
In addition, the Guidelines include a list of criteria that local regulators can use to evaluate whether the right of de-listing was applied correctly. Although DPAs will assess complaints on a case-by-case basis, the list of criteria should be considered as a flexible working tool which, in combination with relevant national legislation, will help DPAs during their decision-making process.

Click here for the full text of the guidelines.

CJEU rules on video recording

Protection of family and property is a legitimate ground for filming

In a preliminary ruling (Judgment in Case C-212/13, referral of the Supreme Administrative Court of the Czech Republic), the EU Court of Justice ("Court") ruled that the personal data protection applies to a video recording made with a surveillance camera installed to a private home but directed towards the public footpath.

Subject to a number of attacks at home, a family installed a surveillance camera to their house which filmed the entrance, public footpath and the entrance of the house opposite to theirs. The camera effectively filmed the moment that a window of the home broke by a shot from a catapult. The recordings made it possible to identify two suspects who were subsequently prosecuted before the criminal courts. As one of the suspects disputed the legality of the video recording, the Court was asked to clarify whether the recording made by the family with a view to protect their lives, health and property fell into the application scope of the Personal Data Protection Directive (95/46/EC).

The Court ruled first that a video recording which covers a public space and which is accordingly directed outwards from the private setting (house) cannot be regarded as a "purely personal or household activity". This means that the requirements and conditions of personal data processing apply in the case at hand. However, the Court ruled in a second instance that legitimate interests may justify the processing of personal data without the consent of the data subject (i.e. the individuals captured by the video). Accordingly, the Court left it to the authority of the national court of the Czech Republic to rule to which extent the filming at hand could be justified on the basis of the legitimate interest of a person to protect his property, health and life.

More information can be found here:
http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-12/cp140175en.pdf

Rights of deceased data subjects in social media

Late October 2014, the French Data Protection Regulator (CNIL) published two articles on the fate of personal data belonging to deceased data subjects, as well as on the rights to those data by their relatives.

The CNIL takes the example of Facebook to emphasize the growing importance of this issue. Currently, one out of 100 Facebook profiles belongs to deceased people, resulting in a

staggering of 130 million affected profiles.
Triggered by the latest regulatory developments on the right to be forgotten and the data portability principle (See the CJEU Google case), the articles open the debate on the concept of “digital death”, its challenges and limitations.
Personal data of deceased persons on social media should also be addressed in the ongoing discussions related to the legitimate expectation to cease active on-line processing of deceased persons vs. family wishes to keep the “digital” identity of the deceased alive, argues CNIL.

The articles of the CNIL also aim at answering frequently asked questions that relatives of deceased persons may have for example on whether they can access an on-line account of the person or transform an existing account to a “memorial” account (e.g. to inform a person’s contacts about the person’s death, etc.). A number of links referring to policies and forms that the social media service providers have published relating to the use of deceased person’s personal data online can be found in the article.

The CNIL articles are available here: Mort numérique : peut-on demander l’effacement des informations d’une personne décédée ? and Mort numérique ou éternité virtuelle : que deviennent vos données après la mort ?

Device fingerprinting subject to user’s consent

On 25 November 2014, the Article 29 Data Protection Working Party adopted Opinion 9/2014 on the Application of the ePrivacy Directive (2002/58/EC) to device fingerprinting (the ‘Opinion’).
The Opinion clarifies that users’ prior consent is required not only in the case of HTTP cookies but also in all cases where online service providers use any technology enabling to single out, link or infer a user or a device over time. According to the Working Party, a number of information elements, for example the media types supported by a browser, may not present a data protection risk *per se* if they are processed in isolation. However, the combination of such elements (especially when combined with the originating IP address) may provide a set of information which is sufficiently unique to act as a unique fingerprint for the device and hence the user of such device.

According to the Working Party, device fingerprinting is increasingly used by online service providers as a substitute to the cookies’ use with the intention to circumvent the user’s prior consent. Allow us to remind once more that the ePrivacy Directive requires a user’s prior consent before providers are allowed to install certain type of cookies on the terminal equipment of users.

The Opinion takes the approach that device fingerprints can also constitute personal data. It further gives a few use cases on the application of the ePrivacy Directive and its exemptions to device fingerprinting.

Click here to consult the full opinion of the Working Party.

Contractual clauses on cross-border data transfers

Making regulators' scrutiny easier?

The Art. 29 Data Protection Working Party studies ways to harmonize and speed up the granting of regulators' permission to contractual clauses that companies usually adopt as a mechanism to protect cross-border data transfers. In many jurisdictions today, the adoption of the standard contractual clauses that has been issued by the EU Commission is not alone sufficient to automatically recognize the transfer as compliant with the European rules on cross-border data transfers. On the contrary, national authorizations are not only required for the use of ad-hoc contracts (not based on the EU standard clauses) but also for the implementation of the Commission's standard clauses. For companies having to submit the same contractual clauses to many local regulators, there is a risk that the latter will not come to the same conclusion as to the "adequacy" of the contractual clauses.

To encounter this risk and based on companies' current experiences, the Working Party has proposed a procedure that will make the mutual recognition of the same contractual clauses by all Data Protection Authorities (DPA) involved easier. The Working Party's suggestion rests on the recognition of a "lead" DPA that will launch and coordinate a "cooperation" procedure amongst the other DPAs, similar to the one proposed for Binding Corporate Rules.

More information can be found here.

Reinforced DPA network for enforcement co-operation

Members of the International Conference of Data Protection and Privacy Commissioners have come to an agreement to develop a secure international information platform. The goal of this

platform is to increase common enforcement action by exchanging information between the members of the DPA International Conference.
This decision was taken at the DPAs conference in October. A report will be made at the 37th annual conference in October 2015.

Click here for the Resolution on enforcement cooperation.

Global automakers commit to enhanced vehicle-based data protection

The Association of Global Automakers have adopted a series of "Privacy Principles for Vehicle Technologies and Service". These Principles commit members of the automotive manufacturing industry to take steps to protect the personal data generated by their vehicles.

The Principles are part of a larger initiative of the automotive industry to enhance the security and privacy necessary to support advanced vehicle technologies and to better protect data in case of cyber-attacks affecting vehicles on the road. While being aware of the numerous benefits of innovative technologies and services, the Global Automakers are mindful of the privacy challenges automated tools involve. Built upon the FTC's work on Fair Information Practices, the ultimate goal of the Principles is to ensure that consumers are consistently protected as long as increasingly more sophisticated and ubiquitous technologies will be embedded in cars.

For more information, click here.

Recent breaches and enforcement actions

News on data breaches appearing in the press during last month:

- Unauthorized access of email addresses and users' passwords from on-line gaming platform in Benelux.
- Cyber-attack on telephone service centers of a Belgian company

Enforcement cases:

- The US Federal Communications Commission (FCC) plans to fine two telecom companies 10 million US dollars for several violations of laws ensuring the protection of phone customers' personal data. These breaches include the storage of customers' sensitive information on unprotected servers.(see FCC - FCC Plans $10M Fine For Carriers That Breached Consumer Privacy)
- The US Federal Trade Commission (FTC) has investigated issues related to the annual re-certification provided by TRUSTe. The FTC has found that TRUSTe failed to conduct this re-certification in 1,000 cases, despite providing information on its website that companies holding TRUSTe Certified Privacy Seals receive recertification every year. (see FTC - TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program)
  The Information Commissioner's Office, UK, has fined a company director for accessing illegally the customer database of a mobile phone company (see ICO - Company director fined for illegally accessing mobile phone company's customer database)

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 HR services company
- Performance of a Privacy Risk Assessment for a company specialized in financial investments
- Assistance to an energy provider in Belgium to understand privacy limitations and conditions in the design of feasibility scenarios relevant to smart meter implementations
- Assistance to a pharmaceutical company to identify data retention obligations relevant to various types of information.
- Assistance to the forensics team of a company of the hospitality sector to understand privacy restrictions related to employee on-line monitoring in several countries, incl. outside of Europe.
- Give dedicated data protection/privacy trainings to the Belgian Financial Sector Federation (Febelfin) and several of its members.

Past & forthcoming interesting events

IAPP Europe Data Protection Congress

The IAPP Europe Data Protection Congress took place in Brussels, Belgium, in the week of 17 November 2014. This 2014 Congress was, according to its organizers the "*most well-attended yet, with a record-breaking number of delegates from around the world*". The Congress covered a wide range of privacy subjects including the latest developments of the EU data protection reform, marketing and big data as well as privacy and technology.

Deloitte presented the benefits of designing data flow maps as a means to better control data flows within an organization and towards third parties. More information can be found here: Multidimensional Data Flow Maps: A Fundamental Building Block of Your Privacy Impact Assessments.

For more information on the 2014 Congress, please visit IAPP Europe Data Protection Congress 2014.

Upcoming events

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