Deloitte.

Belgium | Audit & Enterprise Risk Services | September 2015

Privacy Flash
Belgium

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" 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 current projects taking place.

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

Issue 6
September 2015

EU-US agreement signed

Data protection law enforcement “umbrella agreement” guarantees EU & US citizens same right of judicial redress for breaches

A comprehensive agreement on an EU-US data protection framework was signed on 8 September 2015, covering all personal data exchanged for the purposes of crime prevention and prosecution.

Significant improvements to information rights and data security are included, e.g. purpose limitation, onward transfer and the right to access and rectify. In addition, subject to approval by the US congress, EU citizens will have the same right to seek redress in a US court as US citizens if a US public authority denies a data subject access or unlawfully discloses his or her data.

This agreement complements, standardises and improves existing law enforcement cooperation between the US and different EU Member State authorities.

Read the European Commission factsheet on the “umbrella agreement”.

EU Data Protection Reform

Update

The first trilogue meeting on the EU General Data Protection Regulation (GDPR) took place on 24 June 2015. MEP Jan Philipp Albrecht, Rapporteur for the European Parliament, reported that the participants agree on the fundamental elements of the reform but that many meetings are still required before a final compromise will be reached.

In short, the European Parliament, Commission and Council agree on a number of critical elements serving as the foundations of the reform:

- A single set on rules of data protection, valid across the EU.
- Reinforced rights to put people back in control over their data.
- The same rules for companies across the EU and companies outside the EU.
- A strong and effective one-stop shop mechanism to simplify the lives of companies and citizens.

The European Parliament, Commission and Council also stressed that the 1995 Data Protection Directive is considered to be the minimum level of data protection which needs to be

maintained in the reform. In terms of the fines to be introduced, the Parliament proposed fines up to 5% of annual turnover, while the Council proposed fines upon 2% of annual turnover.

While there is optimism within the European institutions about the progress made so far, the German federal and state data protection commissioners demanded a further strengthening of the Regulation in the areas of data minimisation, purpose limitation and data subject rights late August 2015.

The remarks by Commissioner Jourová on the GDPR trialogue can be found here.

Russian Data Localisation Law

Update

On 1 September 2015, Russia's new data localisation requirement entered into force. The amended data protection law now requires companies from all over the world that collect or process personal data of Russian citizens, to store these data on Russian territory. The entry into force follows a warning shot by the government's IT, telecom and media regulator Roskomnadzor, who briefly blacklisted the Russian-language version of Wikipedia in August.

The same regulator (Roskomnadzor) acts as the Data Protection Authority in Russia and will oversee the enforcement of the new data localisation rules, which seems to be initially aimed at Russian companies. According to reports, large foreign internet companies have been given until 2016 to comply. For 2015, 317 audits have been planned, mostly on Russian companies. However, the regulator plans to conduct inspections on foreign companies with offices in Russia as well, which can result in the blocking of access to the websites of non-compliant organisations.

Earlier reports on the law can be found in previous issues of the Privacy Flash (Issue 1, 2 and 3).

According to information received from our Russian legal correspondents (CMS Russia), the Data Localisation law will most likely have the following practical implications:

- **Operator's obligations:** the law will only affect operators which collect personal data (receive data directly from personal data subjects). Operators may create and actualise a database only in Russia. Personal or depersonalised data may be transferred and stored abroad and can then be further processed according to the rules applicable to the foreign processor. Such transfer of data should have specific and lawful purposes and requires consent of the personal data subject. Furthermore, the law does not make a distinction between operators and processors. Any person involved in processing shall be regarded as an operator and thus subject to the requirements of the law.
- **Duration of personal data storage:** personal data must be destroyed within 30 days after its purpose is achieved unless other deadlines are stipulated by any law which is

binding for the operator. If any law imposes other limits, these required limits shall prevail.

- **Employee data:** the law provides an exemption for personal data processing that takes place for the purpose of pursuing objectives envisaged by Russian law. It is unclear at this point whether the processing of employee data is covered by this exemption. The Ministry of Communications has stated that companies have to assess themselves as to whether their processing could benefit from this exemption and that the regulator will evaluate that decision during inspections. This deviates from an earlier, unofficial position from the regulator (Roskomnadzor), which stated that employee data processing will be subject to the data localisation law.

News

FTC acquires authority to sue companies with inadequate data protection measures

On 24 August 2015, a US appellate court ruled that the Federal Trade Commission has the authority to hold companies accountable for failing to safeguard consumer data. More in particular, the Commission may take legal action against companies engaging in “unfair” or “deceptive” business practices. According to the FTC Act, a practice is unfair when it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition”.

The ruling followed after global hotel chain Wyndham was the victim of three cyber hacks in 2008 and 2009, whereby hackers obtained payment card information from over 619.000 consumers. In short, the FTC is of the opinion that Wyndham “unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft”. For instance, it made use of easily guessed passwords and failed to use “readily available security measures” such as firewalls and encryption to secure its network. On top of that, the company published a privacy policy to ensure its customers that their data is secure and consequently failed to fulfil this promise towards them.

Wyndham argued that the FTC had overstepped its authority in trying to prosecute the company for the data breach, but the court disagreed in its ruling: "A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."

Google declines to comply with CNIL's (French DPA) request to apply the 'right to be forgotten' globally

In June 2015, the French data protection authority, CNIL, requested that Google carry out its delisting on all extensions of the search engine in order to comply with the ECJ decision of 13 March 2014 (the so-called Right to be Forgotten Case). So far, Google has only carried out the delisting on European extensions of the search engine. The delisted web addresses are therefore still retrievable, simply by using Google through the international .com domain or other non-European versions of the search engine.

More information on the CNIL's decision can be found here.

UK DPA approves BCR for CA Technologies

The UK's data protection authority, the Information Commissioner's Office (ICO), approved another BCR in the beginning of July for software company CA Technologies (New York). In order for the BCR to be effective, it has to gain approval from every European DPA in whose jurisdiction a member of the group will rely on them. For CA's view on the approval of the BCR click here.

German DPA (Hamburg) – Facebook

As a consequence to Facebook's attempt to enforce its real name policy, the DPA of Hamburg issued an administrative order against Facebook Ireland Ltd. at the end of July 2015. It appears that Facebook blocked the user's account and asked a user of its website who has used a pseudonym in its Facebook profile to use its real name instead. The operator also requested the person concerned to prove his identity by an official ID photo claiming that the identity document the person had handed over to Facebook was not enough. As the person objected to use his real name, Google unilaterally changed the pseudonym to the real person's name. Following the DPA's decision, the possibility to disable user accounts due to the use of pseudonyms, should be repealed. The decision also stressed that Facebook had to refrain from the unilateral modification of the account to the real name of the user. Accordingly the DPA decided that the actions taken by Facebook violated the "right to use of a pseudonym" enshrined in German Telemedia Act. Moreover, the storage of the digital copy of an official photo ID contradicts the rules of the German passport and identity card law.

Last but not least, the DPA ruled that Facebook had an obligation to comply with German legislation since it is commercially active in Germany through its branch establishment in Hamburg. More information is available at the local DPA's website.

Recent breaches and enforcement actions

- In July 2015, Ashley Madison, a dating site encouraging infidelity was hacked. Users who wished to have their data removed were asked to pay $19 for a “full delete” of their data. However, in a statement published in August, the company confirmed that the data of 36 million users had been released, including the allegedly deleted consumer data. According to the latest news on the matter, the CEO of the parent company of the adultery website has stepped down.
- A university in London has sent out exam results to students by default. After enforcement action from the ICO, the university will introduce mandatory data protection training for all employees handling personal data.
- Also in academia, a number of boxes containing personal information were lost during repair works that took place in a university building. Brunel university will ensure that its staff receives training and enacts additional security measures at the request of the ICO.
- A UK based phone retailer has suffered a cyber-attack that has put customers’ personal data at risk. More information can be found on their website.
- The ICO has fined a firm offering loans, foreign exchange and money transfers following a security breach. The firm lost computer servers with details of several thousand customers.

Deloitte & Privacy recent “wins”

Highlighted below are some of the recent projects our team of privacy and security specialists has been working on:

- Assisting a provider of financial services to understand requirements and restrictions relevant to employee and data monitoring in 17 jurisdictions, including countries outside Europe.
- Assisting a leading international pharmaceutical and biotech company in tackling questions and assignments related to personal data protection at large, as external advisors to the company’s core functions responsible for personal data protection.
- Providing legal support and advice to DG Employment in the set up and implementation of an IT application that EU Member States will use to exchange social security-related information.

- Assisting a cloth manufacturing and marketing company in submitting registrations relevant to an employee compliance ethics tool to local data protection authorities and in adapting the company's global compliance program for enhanced compliance with the EU privacy requirements.
- Assisting a 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 best practices in personal data protection.
- Assisting 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.
- Advising several companies from all industry sectors on the potential impact of the draft EU General Data Protection Regulation and Russia's Data Localisation Law.

- We will also soon be:
  - Carrying out a personal data inventory for a global pharmaceutical company
  - Performing a privacy impact assessment for a national transport network company
  - Reviewing an international bank's privacy tool
  - Providing legal support around data loss prevention to a global biopharmaceutical company.

Forthcoming interesting events

14th Annual Data Protection Compliance Conference

London, UK, 15-16 October 2015
http://www.pdpconferences.com/find-a-conference/82-14th-annual-data-protection-compliance-conference

A 2-day Data Protection Conference held in Central London specifically designed to give Information Professionals the key resources and practical information they need in their daily work.

37th International Privacy Conference

Amsterdam, NL, 26-29 October 2015
https://www.privacyconference2015.org/

The International Privacy Conference is the assembly of all accredited data protection and privacy commissioners from around the world and will be hosted this year by CBP, the Dutch Data Protection Authority. During the conference, the results of the Privacy Bridges Project will be presented. This project was launched in April 2014 on the initiative of Jacob Kohnstamm, the chairman of the Dutch DPA and aims at finding common ground between US and EU approaches to privacy.

European Privacy Academy

http://www.europeanprivacyacademy.com/

The European Privacy Academy is a unique training, knowledge and networking centre focused on the actual day-to-day management of the privacy challenge. It provides both an on-campus data protection officer course and on-campus or in-house department-specific data protection trainings during which attendees learn to efficiently manage privacy and security in a risk based and integrated manner.

The next sessions of the European Privacy Academy are listed below:

DPO Course – October 2015: 27 – 30 October 2015 & 22 January 2016
DPO Course – January 2016: 18 – 21 January 2016 & 15 April 2016

IAPP Europe Data Protection Congress

Brussels, BE, 30 November – 3 December
https://iapp.org/conference/iapp-europe-data-protection-congress-2015/

Training and Workshops: 30 November – 1 December 2015
Conference: 2-3 December 2015

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