Deloitte.

Belgium | Audit & Enterprise Risk Services | July 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 5
July 2015

EU Data Protection Reform

News

The EU's 28 Justice Ministers announced on 15 June 2015 that they reached an agreement on their amendments to the proposed General Data Protection Regulation (GDPR). The Council will now start holding trilogue meetings with the European Parliament and the European Commission, with the aim of finalising the negotiations before the end of the year. A first meeting is planned on June 24th.

The Council's proposal deviates from the Commission's original proposal and the European Parliament's amendments in the following areas:

- **Consent**: the Council has followed the approach of the current EU understanding of consent: consent must be 'unambiguous', and must only be 'explicit' for processing sensitive personal data. The Commission and the Parliament required 'explicit' consent whenever consent is used, which prompted many practical questions.
- **Data Protection Officer (DPO)**: the Council leaves the decision to make the appointment of a DPO mandatory to the Member States. This however does not mean that the situation will remain as it is now (e.g. mandatory in Germany, optional in France, not official in the UK), as several Member States may update their laws to make a DPO mandatory.
- **Accountability, governance & documentation**: Most governance requirements are to be taken on a risk based approach. For example, data protection policies are required 'when proportionate'. Additional emphasis is placed on the use of codes of conducts and certifications to demonstrate compliance. The abolition of the DPA registrations has been kept, but controllers with more than 250 employees do need to keep internal documentation of their personal data processing operations.
- **Data Breach Notification**: The Council proposes that only breaches which are 'likely to result in a high risk for the rights and freedoms of individuals' (examples are provided, such as identity theft) are to be reported to the DPA without undue delay and not later than 72 hours after having become aware of it. The trigger for notifying affected individuals is the same, however without the reference to the 72 hours. This appears to be a more realistic approach, considering the DPAs don't want to be flooded by unimportant breach notifications and the original 24 hours response time would be often impossible to respect.
- **One-stop-shop**: The Council has taken a different approach which would keep more power for the national data protection authority. Only in important transnational cases where several data protection authorities are involved, companies making business in more than one EU country will only have to deal with one single supervisory authority. In case of a local data protection issue, the subsidiaries of the company will be in contact with its local authority.
- **Fines**: The Council has returned to the approach of the Commission: a tiered fining system, which would lead up to maximum fines of 1 million EUR or 2% of the total worldwide turnover of the preceding financial year. The infractions in the highest tier include processing without consent, not notifying a data breach or not conducting a privacy impact assessment. While 2% is lower than the 5% proposed by the Parliament, it doesn't change the fact that stellar fines will in all likelihood be possible as of 2018.

The announcement follows the issuing of a preliminary timeline for the trilogue meetings by the EP's largest political group EPP. If the EU's lawmakers stick to this timeline, the EU's 20 years old patchwork of data protection laws will be replaced by a unified regime by the end of 2017/early 2018.

News

Data breach notification now mandatory in the Netherlands

Despite the EU's seemingly unwithered commitment to finalising the new Data Protection Regulation (GDPR) by the end of 2015, Dutch lawmakers have taken matters into their own hands. On 26 May 2015, the First Chamber passed a law that will make the notification of data breaches to the Dutch Data Protection Authority (CBP) mandatory and subject to heavy fines.

The Bill on Data Breach Notifications (*Wet Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp*) obliges data controllers to notify the CBP of any security breaches that have or are likely to have serious adverse consequences for the protection of personal data. The CBP will issue guidance at a later stage to help controllers determine when the consequences of a breach should be considered serious.

In addition to notifying the DPA, the individuals whose data were compromised in the breach should also be informed, unless the data are unintelligible to third parties or encrypted.

The bill gives the Dutch DPA the power to issue fines of a maximum of €810,000 or 10% of the company's annual net turnover for every violation. You may wish to read the analysis of the new law that was recently issued by our colleagues at Deloitte Netherlands (in Dutch).

Belgian Privacy secretary to propose increased DPA powers

Belgian State Secretary for Privacy Bart Tommelein recently announced his intention to introduce a bill after the summer that would reform the Privacy Commission into a full-fledged regulator with fining powers. Tommelein cited the example of the Dutch DPA (see above), which can now issue fines of up to €810,000. In order to fulfill this task, the State Secretary acknowledged that the Privacy Commission would also need an increase in manpower and funding.

Data retention law abolished by Belgian Constitutional Court

Privacy groups in Belgium celebrated a legal victory this month, as the country's Constitutional Court struck down its data retention law. The law, which transposes EU Directive 2006/24/EC, obliges telecommunications service providers to retain metadata on voice and data traffic for one year. The Belgian League for Human Rights and the Francophone Order of Lawyers had started a procedure at the Constitutional Court in order to have the law repealed. The Court has now followed their pleas.

The decision follows similar developments in other EU Member States: both in Germany and in the Netherlands, data retention laws had already been repealed. The European Court of Justice declared last year that the EU directive, on which all three laws were based, is invalid, as the "serious interference" into privacy goes beyond what is strictly necessary. The Belgian Constitutional Court followed the same reasoning.

Drones

Article 29 Working Party issues opinion on drones

The EU's independent data protection advisor, the Article 29 Working Party, last month issued an opinion on the privacy and data protection issues that arise from the increase use of drones by both public and private operators.

The Working Party recognizes that several privacy risks may arise in relation to the processing of personal data carried out by a drone's on-board equipment, especially when used for law enforcement purposes. In order to address these concerns, the Opinion provides clear recommendations to manufacturers, operators, law enforcement and policymakers/regulators.

Concretely, the Working Party recommends operators and manufacturers to abide to the principle of privacy by default and by design, setting up on-board technology in a way that avoids the collection and/or further processing of any unnecessary personal data. In addition, operators should look for the most appropriate way to give advance notice to those who could be impacted by the drone's data processing: through signposts, relevant websites, social media, etc.

On the use of drones for law enforcement, the Working Party also emphasized the importance of the transparency principle. The use of drones should be prescribed by law and the data subjects should be informed of the processing in as far as possible. In any case, the use of drones should not allow for constant tracking of individuals.

Study

Majority of American consumers disagrees with privacy trade-offs

Coinciding with Apple CEO Tim Cook's comments about free online services such as Google's new Photos service, a study from the University of Pennsylvania pointed out that American consumers do not think that trading their privacy for free or personalised services constitutes a fair deal.

Presented with statements such as "If companies give me a discount, it is a fair exchange for them to collect information about me without me knowing", a majority of respondents disagreed or disagreed strongly. According to the authors, the study reveals that a majority of Americans 'do not want to lose control over their information but also believe this loss of control has already happened'.

For further reading, we refer to the New York Times article "Sharing Data, but Not Happily", which features both Tim Cook's comments and the main findings of the study.

Privacy Enforcement

France DPA to conduct more privacy audits in 2015

The Data Protection Authority of France, the CNIL, issued a statement at the end of May announcing its intention to conduct 550 inspections of firms' privacy practices this year. 350 of these will take place on-site; the rest will be conducted online.

The CNIL will focus more specifically on contactless payments, the protection of employee data, and the monitoring and sharing of health data gathered via mobile apps and devices. In addition, the 68 multinational companies that have had their Binding Corporate Rules (BCRs) approved by the CNIL can expect an audit this year.

Last year, the French watchdog conducted 421 inspections, of which 58 were online audits. It issued 62 enforcement notices and 18 penalties in 2014, including 8 fines.

If the FTC comes to call

In a recent blog post, the Federal Trade Commission, the US consumer watchdog, details what companies can expect when they are the target of an FTC data security investigation. The FTC is amongst others responsible for ensuring that companies process consumer data securely and in accordance with privacy regulations, including the EU-US Safe Harbor Framework.

The blog post emphasizes that investigations start informally: by reading the organisation's website and possibly reaching out to the company directly with regards to their privacy and security practices. If the FTC decides to proceed with a formal investigation, it issues a request for information. The focus of the information gathering is on what policies are in place and whether they are actually enforced, and whether the company's practices are "reasonable in light of the sensitivity and volume of consumer information the company holds".

Belgian Privacy Commission starts proceedings against Facebook

After the results of a study performed by iMinds, Free University Brussels and KULeuven indicated that Facebook does not comply with European and Belgian privacy law, the Belgian Privacy Commission started litigation against the social media giant on 14 June 2015.

The Privacy Commission had presented its findings to Facebook in May already and highlighted particular concerns with the company's tracking of non-users. In response to the news about the litigation, Facebook asked the Commission to stop proceedings, in order to continue talks on different aspects of its privacy policy. The Privacy Commission however considers the court case and the discussions with Facebook to be separate and not mutually exclusive.

It is the first time that Facebook is challenged in front of a court by a European DPA.

Deloitte & Privacy recent "wins"

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

Performing a privacy risk assessment for the entire operations of one of Belgium's leading car leasing firms.

- 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 best 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 the potential impact of the draft EU General Data Protection Regulation and Russia's Data Localization Law.

Forthcoming interesting events

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

Homepage

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