Privacy Flash – Issue 25

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 is to provide monthly updates on global regulatory developments, as well as relevant news and information on upcoming events in the field of data protection and privacy.

Previous issues are available on our website, via the 2015 | 2016 | 2017 | 2018 archive

For additional information, to subscribe, or to suggest improvements to the Privacy Flash, please email BEPrivacyFlash@deloitte.com.

To unsubscribe, please send us an email using this link.

Highlights

- 25 May 2019: One year with GDPR
- EU privacy supervisory authorities release their 2018 reports
- Deloitte survey – Maintaining the momentum – GDPR 10 months on
25 May 2019: One year with GDPR

The first year of enforcement of GDPR is over and leaves a positive record. After the first lessons learnt, oversight authorities and companies appear better prepared to continue their investments towards sustainable compliance during this year and the next ones to come.

Below is the summary of a few reports that the EU and national data protection regulators have recently issued. They outline the main activities that kept the EU and the national DPA busy last year, while providing perspectives of DPAs’ plans for the coming months and onwards.

As the reports show, citizens are also better informed about their rights, although they may still feel the lack of “user centricity” and mechanisms to help them exercise these rights effectively. This conclusion aligns with the results of the latest public survey that Deloitte Belgium conducted on GDPR. The encouraging message is that companies have already invested in mechanisms and technologies to accelerate their compliance efforts. The survey shows that these efforts must however continue as there are still quite some important areas for which the market feels the need for improvement.
EU privacy supervisory authorities release their 2018 reports

The European Data Protection Supervisor (EDPS)

2018 Record

In its annual 2018 report, the EDPS proudly lists the following topics as key achievements attained during that year:

- **Preparing for a new legislative framework**
  Invested in the launch of the European Data Protection Board (EDPB), the GDPR preparation and in encouraging the adoption of the new ePrivacy Regulation (still a draft).

- **Relation with Europol**
  Confirmed their role of supervisory authority of Europol, built on a strong working relationship towards striking the right balance between privacy and security in the context of law enforcement. The regulator also informed that they become the supervisory body for Eurojust as from now onwards.

- **Security and EU borders**
  Contributed to several policy proposals relating to EU border security and fostered co-operation with other EU institutions and national authorities for the coordinated supervision of processing activities in border control systems currently in place, such as SIS II, VIS and Eurodac.

- **Data protection for EU institutions**
  Focussed on enhancing EU institutions and bodies’ readiness to comply with the new data protection rules as set out in Regulation (EU) 2018/1725 (equivalent law to GDPR for EU institutions).

- **International landscape**
  Continued the close collaboration with their data protection partners around the globe to assure an ever more international approach to data protection policy. Commitment to keeping the momentum on the topic of digital ethics through the organisation of many initiatives (e.g., web-streamed conversations and podcasts, on-line publication of thought-leaders on the issue, a new EDPS opinion on ethics).

2019 Objectives

The EDPS’ 2019 objectives are to continue the interaction and dialogue with the EDPB, international organizations and DPA to promote a global presence of data protection rules. Amongst the key priorities of 2019 are:

- Enhance the understanding of the new data protection rules and the principle of accountability.
- Invest in new policy and consultation activities: With the entry into force of Regulation (EU) 2018/1725, the European Commission is explicitly required to consult the EDPS in specific cases. EDPS also has the ability to issue joint opinions with the EDPB. Accordingly, EDPS is committed to fostering intra-institutional cooperation in these areas by investing in these new competences.
- Provide guidance on necessity and proportionality: the completion of the Necessity Toolkit that provides guidance on necessity and proportionality is on
track. The Necessity Toolkit already includes guidelines regarding records, registers, DPIAs and prior consultations.

- Promote interoperability: A wider debate on interoperability between the EU's large scale IT systems was launched.
- Conduct effective oversight: the intention is to continue to conduct inspections focused on technological aspects, in particular those relating to large-scale IT systems and those in the area of security and law enforcement.
- Work on data protection by design and by default in the EU institutions: efforts must be increased to identify and promote practical technological solutions through better monitoring of ICT developments in this area; the practical goal is to establish guidance and to provide training on the technical implementation on data protection. Support to the Internet Privacy Engineering Network (IPEN) will continue.
- Provide guidance: this objective aims at enhancing accountability in IT. EDPS will encourage guidance on specific technologies and methodologies, with emphasis on IT security. Where feasible, the EDPS envisages doing this remotely from the EDPS lab.

**National Data Protection Authorities (DPA)**

**AP - Autoriteit Persoonsgegevens**

The Dutch DPA (Autoriteit Persoonsgegevens, AP) is the first Data Protection Authority in the Benelux to have published its 2018 annual report. The AP reorganised itself to continue being able to meet expectations with the increase of tasks and responsibilities for DPAs.

**Activities in 2018**

**European Cooperation**

The GDPR aims to harmonise the privacy rules within the EU. The European Data Protection Board (EDPB) plays a central role in the cooperation and consistency mechanism guaranteeing uniform application of the GDPR within the EU. The AP participated actively in the EDPB, for example by acting as reporter in meetings or subgroups and by taking the lead in drafting guidelines.

Cooperation with other Data Protection Authorities took place through the one-stop-shop mechanism, where the AP acted as Lead Supervisory Authority in 69 international cases and was otherwise involved in 342 cases. While in 2018 there were no examples of joint operations as described in article 62 of the GDPR, the AP generously provided mutual assistance on 15 occasions and requested mutual assistance in 9 instances under article 61.

The AP continued its participation in several European monitoring groups in the area of freedom, security and justice, covering Europol, Eurojust and European information systems such as the SIS II.

**Awareness, informing and practical advice**

A key aspect of the 2018 activities of the AP was raising awareness, providing information and offering practical advice to both data subjects and organizations regarding their rights and responsibilities under the new regulation. Furthermore, the AP also published practical information on the GDPR, for example on wi-fi.
tracking and direct marketing. The AP also worked closely with DPOs, while advising in parallel the Dutch parliament, for example on the topic of internet service providers.

**Regulatory oversight and actions**

The AP received more than 11,000 complaints related to the handling of personal data. About a third of these complaints concerned the rights of data subjects, especially the right of access and the right of erasure. The responses to these complaints predominantly encouraged corrective measures be taken by organisations processing personal data. In the future, the AP plans to react more increasingly to complaints with investigations and sanctions.

In the first year of the GDPR's entry into force, the AP focussed its investigations in the public and the health care sectors, personal data trading activities and data breaches. Regarding the sectorial investigations, the AP focused on compliance with accountability obligations for instance by verifying whether organisations have appropriately registered the appointment of Data Protection Officers (DPO) towards the authority. The AP also highlighted a few of its high-profile cases: it discovered that the privacy of Windows 10 users (of which there are approximately 4 million in the Netherlands) was not sufficiently protected. Microsoft promised to fix the issues during an update in April 2018. As the proof of the pudding is in the eating, the AP is currently investigating whether Microsoft's update did effectively contain the necessary corrective measures.

Another case concerns Facebook, who was considered to have insufficiently informed their 9.6 million users in the Netherlands about the processing of their data, for example for the purpose of personalised advertisements. After the intervention of the AP, Facebook adapted their privacy policy in April 2018. The AP has referred the case to the Irish Data Protection Commission who as Lead Supervisory Authority is in charge of investigations regarding Facebook.

Last year, 20,881 data breach notifications were submitted to the AP, which doubled the 2017 figures. Worth noting is that Uber was imposed a fine of 600,000 EUR for delaying the reporting of a data leak that took place in 2016 and affected 57 million users.

The AP reported a noticeable increase in new requests for approval of Binding Corporate Rules (BCR) from 5 requests in 2017 to 32 in 2018.

**2019: the road ahead**

The past year, AP invested in informing and advising, instead of taking ‘punitive’ actions such as investigations and administrative fines. The AP also restructured its organisation, obtained legal personality and increased its headcount with 60 FTEs to a total of 157 FTEs. It is needless to say that the reorganisation and growth has been one of the main challenges the Dutch privacy regulator faced last year.

While in 2018 the AP’s focus mainly concerned developing a collaborative approach towards companies and citizens especially in the area of breach reporting and implementation assistance, its objective this year is to optimize internal working processes, develop its risk-based approach and achieve the right balance between preventive, corrective and repressive instruments by expanding the authority's law enforcement actions.
Key take aways

During 2018, the AP has invested significantly in reinforcing its internal resources and confirmed its advisory and awareness-raising role towards the market and the citizens. On an international level, the Dutch data protection regulator already shows a good record of EDPB participation and cooperation with other DPAs. More is planned for this year especially in the area of investigations and enforcement by adopting a risk-based approach.

CNIL - Commission nationale de l'informatique et des libertés

Along the same lines, the French DPA (Commission nationale de l'informatique et des libertés, CNIL) outlines the following as key actions of its 2018 record:

- **Support to the citizens**
  The CNIL received about a third more complaints in 2018 (11,077 in total) as compared to 2017. The vast majority of complaints concerns national data processing activities, with only a fifth of them being handled in cooperation with the other European Supervisory Authorities. Increased awareness of data subjects translated into more data deletion requests and the application of data portability in the banking and online content services. Citizens’ awareness on remote viewing of CCTV images and cameras’ installation were also extensively covered in the authority’s awareness last year.

- **Support to professionals**
  Companies and other organizations consider CNIL as an authoritative source of information, resulting in increased user traffic on the CNIL’s website (+ 80%) and a 22% increase of phone calls received. Without providing specific numbers, the CNIL also invested in tools being widely available to support organizations, such as for instance the DPIA tool that the authority made available online in 18 languages as well as the massive open online courses on the website.

- **Enforcement actions**
  During the year, the CNIL conducted 310 investigations, most of which (204) concerned online controls. One in ten of those concerned CCTV system investigations, highlighting the particular sensitivity of the country on this topic. With its 49 orders, the CNIL targeted in particular the insurance sector (5 orders) and the advertising technology sector (4 orders). Ten monetary sanctions and a non-public warning were also issued.

On its agenda 2019-2020, the authority will work, amongst others, on:

- **Education and dissuasion**
  The CNIL considers GDPR as a keystone of a trusted digital environment. Its actions will be focussed on market education and dissuasion. Smaller and less mature organizations can expect awareness support, in the form of specialized publications and additional privacy compliance tools. The other side of the coin, dissuasion, is considered as a necessity for the credibility of the GDPR. Even when applying sanctions, the goal of the CNIL is to make business models evolve and become more privacy-friendly.

- **Infrastructures and platforms**
  As it has already done with publications on Blockchain and connected cars, the CNIL aims to remain on top of technological evolutions and their potential impact on privacy.
Diplomatic actions
On a European and international level, CNIL intends to continue its leading role, particularly in the framework of the 2019-2020 work program of the European Data Protection Board (EDPS). Beyond Europe, the main aim is to obtain a convergence of data protection principles worldwide.

GBA - Gegevensbeschermingsautoriteit

The Belgian DPA (Gegevensbeschermingsautoriteit, GBA) did not lag behind either and also published the following as key accomplishments of year 2018:

- Development of new electronic forms
  The creation of an electronic registration form for the communication of a DPO and the electronic data breach notification form.

- Exercise of control activities
  Since 25 May 2018, the Inspection service of the GBA conducted control activities through periodical monitoring and thematic inspection assignments on (inter)national processing activities in the public and private sector, based on a risk approach. In the 4th quarter of 2018, 70 investigation files, of which 67 originating from complaints, were submitted to the Disputes chamber of the GBA. The most important complaints related to the functioning of cities and municipalities and the local elections of 2018, the use of cameras and the new camera legislation and the functioning of governmental or administrative bodies.

- Dispute resolution
  During the same period of time, the Disputes chamber handled 100 complaints. In some cases, additional research was ordered, while in other cases the data controller was asked to satisfy the data subject requests asked. One complaint was transferred to the public prosecutor’s office in Brussels, due to the nature of the facts. The most recurrent topics of the complaints were relating to the local elections of 2018, the use of CCTV, including on the workplace, the writing of newsletters and the lack of lawfulness and proportionality of processing activities.

- Handling of requests to first-line support
  The first-line service of the authority received and treated 6,491 core cases (requests for information, arbitration, data breaches and control files) throughout the year, which is 66% more than in 2017. It received for example 429 personal data breach notifications, compared to only 17 in 2017. In all cases, the data subject was first requested to contact the data controller, before the authority undertook action against the controller. The top 5 “hot” topics on which advice was asked were data subject rights, general GDPR-questions, questions on surveillance cameras, direct marketing and notifications.

- GBA’s Knowledge center
  The GBA’s Knowledge Center issued advice in numerous areas such as police, justice and safety, administrative simplification, economic matters and governmental matters, certification and accreditation, as well as codes of conduct.

- Education and awareness
  The ‘I decide’ project was put in place, aiming at enhancing the privacy and data protection awareness, in particular where it concerns children and young people by stimulating their ‘privacy-reflex’. Yet, the content of the website is tailored to the needs of other target groups close to the children and youth, such as parents and teachers.
Deloitte survey – Maintaining the momentum – GDPR 10 months on

A few months after the entry into force of the General Data Protection Regulation (GDPR), Deloitte Belgium conducted a survey to gain insights into the attitude and expectations of organisations and consumers in Belgium with regard to data protection. The survey reached a wide range of businesses from all industry segments and sectors (financial and healthcare, consumer services, IT and the public sector).

Key Survey insights

- **Territorial scope**
  The extended territorial scope of the GDPR has had a clear impact, as there has been equal focus by organisations inside and outside the EU on the topic of personal data compliance.

- **Trust is a key**
  Ethical use of data is perceived as an increasingly important driver of consumer trust. When individuals trust organisations, they share their data more openly and are less likely to leave or challenge an organisation if it suffered a breach or exercise their data subject rights.

- **Consumer centricity**
  Awareness of privacy is increasing, but more customer centricity is necessary to increase individuals’ control over their data. However, individuals still pay little attention to privacy notices while GDPR programmes may have been too focused on internal compliance rather than taking a consumer centric view.

- **Data subjects’ requests**
  Respondents experienced a large rise of all access request types. Although the most commonly received requests concern data portability, only 35% of survey participants are confident in their ability to respond to those in time.

- **Required resources**
  85% of the organisations mention having the required resources to support sustainable GDPR compliance. From the 15% of them who lack the required resources, 6% are actively recruiting and/or trying to create budget.

- **Key drivers for compliance**
  According to the views gathered, these are the three key drivers for compliance are reputation (82%), increased consumer trust (65%), regulatory actions though not necessarily fines (53%).

- **The way forward**
  In terms of long-term compliance, 94% of organisations claim confident in demonstrating their ability to comply with GDPR and more than half of them used internal and external tools in order to achieve this (61%). Yet, sustainable compliance is still an issue (with only 15% having adequate resources to do so).

- **Technological investments**
  Until now, 6% of the participating organisations have used existing technologies, while 27% have developed internal technologies and 21% used external tools. Figures vary per compliance area (data subject rights, records, data leakage prevention (DLP) tools and so on).

- **Important concerns**
  Data usage for marketing purposes and data security when implementing new processes are ranging first. This is followed by hacking and its negative reputational effects. A third concern relates to awareness and cultural change within the organization’s environment.
In a nutshell, the GDPR has triggered positive action amongst business, while the reporting on GDPR compliance and the confidence of an organisation’s ability to demonstrate compliance are steadily increasing. There is still room for development in areas such as consumer centricity, cyber-risk prevention, awareness, cultural shifting, in other words: in sustainable compliance.

A leading audit and consulting practice in Belgium, Deloitte offers value added services in audit, accounting, tax and legal, consulting and financial advisory services.

In Belgium, Deloitte has more than 4,000 employees in 13 locations across the country, serving national and international companies, from small and middle-sized enterprises, to public sector and non-profit organisations. The turnover reached 510 million euros in the financial year 2018.

Deloitte Belgium CVBA is the Belgian affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited. We are focused on client service through a global strategy executed locally in more than 150 countries. With access to the deep intellectual capital in the region of 286,000 people worldwide, our member firms (including their affiliates) deliver services in various professional areas covering audit, tax, consulting, and financial advisory services. Our member firms serve over one-half of the world’s largest companies, as well as large national enterprises, public institutions, and successful, fast-growing global companies. In 2018, DTTL’s turnover reached over $43.2 billion.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© 2019. For information, contact Deloitte Belgium.

To no longer receive emails about this topic please send a return email to the sender with the word “Unsubscribe” in the subject line.