Privacy Flash – Issue 20

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 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

- ePrivacy Regulation: EU Council amendments
- Bărbulescu case: Final decision
- UK: Draft government bill
- Poland: Draft GDPR law
- GDPR: ICO public consultation
- FTC enforcement actions against non-compliant privacy participants
- Belgian Data Protection Authority
- CNIL's public consultation
- French court refers Google privacy case to CJEU
- Canadian Data Protection Authority annual report

News

EU Council proposes amendments to the draft version of the ePrivacy Regulation

As reported in Privacy Flash issue 18, the European Commission published a proposal for a regulation on the confidentiality and privacy of electronic communications, aiming to replace Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (the "ePrivacy Directive"). The goal of the proposal is to extend the current rules on privacy and data protection to all forms of electronic communications, regardless of them being offered by a telecommunications provider or an "Over-the-Top" communications service provider, such as Skype, WhatsApp or Facebook Messenger.

Recently, on 8 September 2017, the EU Council published its proposed revisions to the draft version of the ePrivacy Regulation of the European Commission. The introduction of the file note states that the "revisions are based on the discussions held in the meetings of the Working Party for Telecommunications and Information Society ("WP TELE") and are without prejudice to any comments delegations might wish to make in the future". It also states that the "redraft of the EU Council aims mainly at clarifying certain elements and at outlining specific issues to be examined for the purposes of advancing the discussions on the file".

The revisions of the EU Council focus on the articles of the proposal. The recitals will be examined at a later stage. The proposed amendments of the Council include, among others:

- Clarifications on the precise material and territorial scope of the Regulation;
- Streamlining of the provisions on representatives, bearing in mind the corresponding provisions of the General Data Protection Regulation (GDPR);
- Relocation of the provision on consent to the general part since it applies to the whole Regulation;
- Simplification of the wording of the consent provision in art. 4a of the Regulation;
- Aligning the conditions for valid consent with art. 10 of the Regulation and with the GDPR;
- A new provision allowing the possibility of collective redress (so-called "class actions") for end-users who are natural persons, to ensure consistency with the GDPR.

Furthermore, WP TELE meetings took place on 19, 20 and 25 September 2017, during which the Presidency discussed the proposal and its proposed changes article-by-article. During these discussions, delegations were invited to express their views on these proposed changes.

Final decision in the Bărbulescu case: Grand Chamber protects employees' workplace privacy

In a continuous evolving area of law concerning technology, privacy and workers' rights, the Grand Chamber of the European Court of Human Rights decided to come back on an earlier decision by its Chamber, and enhance privacy protection for employees' private electronic communications such as emails. As modern day-

to-day communications blur the boundaries between work and spare time, this judgement is of significant importance.

In its original ruling on the Bărbulescu case on 16 January 2016, the Chamber of the European Court of Human Rights (ECHR) decided that an employer was allowed to monitor his employees' emails. In its decision, the Court tried to strike a fair balance between, the employees' right to respect for his private correspondence on the one hand the employers' right to verify whether employees comply with internal security policies on the other hand. The judgement ruled in favor of the employer as it was "not unreasonable for an employer to want to verify that employees are completing their professional tasks during working hours". Moreover, the internal company policies clearly prohibited all private use of the professional email account. The Court decided that Mr. Bărbulescu's right to respect for his private life and correspondence was not violated.

However, the recent decision of the Grand Chamber on 5 September 2017, overturns the previous judgement and strengthens employees' privacy. In contrast to the initial ruling, the Court decided that the company policy was too general and vague. Mr. Bărbulescu had "not been properly informed in advance on the extent and nature of his employer's monitoring, or the possibility that the employer might have access to the actual content of his messages". If an employer wants to monitor employees, a detailed monitoring policy needs to be in place which sets out parameters on why, how and where an employer performs the monitoring.

The final decision in the Bărbulescu case indicates that the right to privacy in the workplace does exist. Certain European countries already introduced legislation on the issue of workplace privacy. Most of these domestic regulations require employers to give notice prior to starting any monitoring activities. However, in many cases this prior notification may not be enough. Additional parameters such as the extent of the monitoring, the absence of less intrusive measures, the legitimate reasons and the presence of adequate safeguards should be taken into account.

UK introduces draft government Bill

On 14 September 2017, the UK Government published a first draft of the Data Protection Bill. This Bill is intended to replace the current Data Protection Act 1998 and to implement the new EU General Data Protection Regulation. It also seeks to incorporate provisions of the Law Enforcement Directive (2016/680).

The Data Protection Bill intends to adapt UK's data protection law to the digital age and increase the level of control people have over their data. With this bill, the Government also wants to make sure that the UK's Data Protection Law can properly function despite the UK's departure out of the EU.

The Bill addresses five keys elements:

- **General processing**: Part 2 of the Bill incorporates the provisions of the General Data Protection Regulation and institutes the standards for general data processing.
- **Law enforcement processing**: Part 2 does not apply to the activities carried out by law enforcement authorities. Hence, Part 3 introduces standards for Law Enforcement Processing. It includes provisions specific to the processing of personal data by any competent authorities for any law enforcement purposes.

- **Intelligence services processing**: Part 4 relates to National Security Processing. This part refers to rules that must be applied for any national security processing, including the processing of personal data by intelligence and security actors.
- **The Information Commissioner**: Part 5 covers the role of the Information Commissioner, the supervisory authority in the UK, which was established under the existing Data Protection Act 1998. The Data Protection Bill ensures that this role continues to exist under the new act. The Bill gives the Information Commissioner investigative, advisory, corrective and authorization power.
- **Enforcement**: Part 6 aims at ensuring the enforcement of the rights under the Bill. In the case of serious data breaches, data controllers and processors will be subject to a fine up to 20 million euros or 4% of the global turnover, or 10 million euros or 2% of the global turnover. The Bill also sets up new criminal offences dealing with emerging threats.

Moreover, Schedules 2, 3 and 4 of the Bill provide exemptions from the GDPR. Restrictions on data subject rights are possible for reasons relating to freedom of expression, scientific or historical research purposes, statistical purposes and archiving purposes, etc.

The Bill was first introduced to Parliament on 14 September 2017 and is currently going through the Committee stage in the House of Lords.

Poland issues draft GDPR implementation law

With the aim to make national law compliant with the GDPR, the Polish National Legislative Center has issued a package of draft laws, including the amended draft of the act on personal data protection. The draft law sets forward the powers of the Polish Data Protection Authority (Office of Personal Data Protection) including amongst others investigative power and the power to publish recommendations stating the technical and organisational measures that ensure personal data is processed securely.

The package, consisting of 175 pages of legal text and 145 pages of justification for the proposed alterations, introduces a big change to the current framework. For a period of 30 days, the draft laws will be open for public consultation by over 200 business representatives and associations.

Multiple sectors (digital, energy, infrastructure, culture, finance (incl. banking and insurance), employment, sports and tourism, health and justice) are subject to the new data protection rules. In terms of employment, processing of personal data (including biometric data) by the employer will only be allowed in the context of existing employment relationships, and where the employee has given consent, either electronically or in writing. Furthermore, financial institutions are entitled to process personal data of their clients, including profiling, in order to assess creditworthiness and credit risk analysis.

The new legal framework is expected to become binding before May 2018. It remains to be seen how the business will comment during the period of public consultation and the changes this may bring.

ICO opens public consultation on its GDPR guidance on contracts between controllers and processors

On 13 September 2017, the Information Commissioner's Office (ICO) opened a public consultation for its draft guidance on contracts and liabilities between controllers and processors under the GDPR. The GDPR now stipulates that a written contract or other binding legal act is required whenever a controller engages a processor for data processing purposes. This obligation ensures that the responsibilities and liabilities of each parties are clearly set out and understood by all parties involved. The draft guidance aims to address the varied provisions these contracts are required to contain.

According to the guidance, contracts must incorporate details regarding the processing of the data including the subject matter, the duration of the process, the nature of the processing, its purpose, the type of personal data, categories of data subject and the obligations and rights of the data controller. Contracts musts also include terms defining the obligations of the processor.

The Guidance also determines the controller's responsibilities and liabilities. The controller has the responsibility to choose a processor that can ensure that the requirements of the GDPR will be met and that the rights of the data subjects will be respected. The controller will therefore be liable for any damages arising from an infringement of the GDPR. The only way for the controller to decline liability would be to prove that it is "not in any way responsible for the event giving rise to the damage".

Processors are also subject to their own responsibility and liability. They will have to pay damage if their obligations under the GDPR are not met or if they act outside their controller's instructions.

The consultation on the draft guidance was closed on 10 October 2017. No date for publication of the finalized guidance has been released yet.

FTC brings first enforcement actions against non-compliant Privacy Participants

On 8 September 2017, the US Federal Trade Commission (FTC) reported to have settled charges against three companies, accused of misleading consumers about their involvement in the European Union – United States Privacy Shield Framework. The Privacy Shield Framework enables companies to legally transfer personal data from the European Union to the United States. The EU-US Privacy Shield Framework was adopted in 2016, replacing the former EU-US Safe Harbor Framework.

The FTC filed several individual complaints against Decusoft, LLC, Tru Communication, Inc. and MD7, LLC, accusing these companies of falsely claiming certification under, and thus violating, the Privacy Shield Framework.

The role of the FTC is to ensure that companies maintain their promises upon joining the Privacy Shield Framework. With the previous US-EU Safe Harbor Framework, the FTC already brought forward 39 enforcement actions. These more recent actions follow the enforcement actions the authority launched related to the Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System.

With these enforcement actions, the FTC wishes to assure that companies are liable for their promises made to their consumers with respect to their privacy policies. These actions illustrate the FTC's intention to aggressively enforce the Privacy Shield Framework, which has been put in place to facilitate transatlantic commerce and the corresponding personal data flows.

Following their settlement with the FTC, the three aforementioned companies agreed to stop misrepresenting the extent of their participation in any privacy and security program funded by the US government. The order will be valid for a period of 20 years.

Belgian Data Protection Authority under reform

The establishment of the Belgian Data Protection Authority (DPA) dates back to 1992 and is therefore no longer adapted to the European Market and digitalised world. A reform is needed in order for the DPA to be able to fulfil its role in a new environment. Hence, the Belgian Chamber of Representatives published a bill, which aims at reforming the Belgian DPA. The main goal of the bill is to align the DPA with the new rules and obligations as set out in the General Data Protection Regulation (GDPR).

Where in the past the DPA had more of an advisory role and little enforcement power, this will now change. The future DPA will have strong monitoring powers and the ability to impose direct administrative fines if necessary. The structure of the future DPA will consist of six different subparts: a management committee, a general secretariat, a first line service, a knowledge center, an inspection division and a dispute settlement body. Management will be reduced to five permanent and full-time mandatories. These measures should increase the professionalism within the DPA.

The DPA will receive several new competencies and roles. These can be divided into four different categories:

- **Advisory role**: Giving information and advice to private entities, data controllers and policymakers on how to comply with data protection legislation.
- **Encouraging role**: Encourage data controllers and processors to utilise preventative instruments, as foreseen in the GDPR, as much as possible.
- **Audit role**: Auditing data controllers and processors for compliance by a specialised inspection division.
- **Sanctioning role**: Imposing sanctions in situations where data protection legislation is violated. These sanctions can vary from formal warnings to fines.

By introducing this bill, the Chamber hopes to create a modern DPA with strong competences. This reform should allow the DPA to effectively verify compliance with data protection legislation and to better protect consumers and civilians when confronted with new technologies.

Transparency and international data transfers, topic of the CNIL's public consultation

The French Data Protection Authority, CNIL, launched a public consultation on 19 October 2017, regarding two key topics of the GDPR: transparency and international data transfers. The consultation follows two prior consultations on data protection officers, right to data portability, data protection impact

assessments and certification on the one hand; and the concepts of consent, profiling and incident management on the other hand.

Being subject to the Article 29 Working party's 2017 action plan for implementing the GDPR, the purpose behind the CNIL's online consultation is to gather stakeholders' concerns and issues on the GDPR and to feed them into the Working Party's preparation of the guidelines on these concepts.

Along the same line, the Irish Data Protection Commissioner has issued a public consultation on the same topics that was open until 13 October 2017. The outcome of both consultations were subject for discussion during a "FabLab", organised by the Article 29 Working Party on 18 October 2017.

French court refers Google privacy case to CJEU

In a recent decision, France's highest administrative Court – le Conseil d'état – has referred a case concerning Google and the so-called right to be forgotten to the Court of Justice of the European Union (CJEU). In a previous judgement (see previous Privacy Flash issue), the CJEU decided that citizens have the right not to appear in search results of online search engines such as Google or Bing if certain criteria are met.

The question now is whether this previous judgement must be extended to worldwide search requests. In other words, is Google required to extend the right to be forgotten on its search domains situated outside of the European Union (e.g. google.com)?

This debate traditionally puts two groups of people up against each other. On the one hand, privacy advocates are convinced that individuals are in need of greater control over their online information. Whereas for the proponents of freedom of speech, this extension would entail a way of censorship which cannot be tolerated in a modern online society.

According to Google, each country should be able to define for itself what kind of online information is accessible for the data subject. It further states that there should be a fair balance between people's right to privacy and the freedom of expression. France's privacy watchdog – la Commission Nationale de l'Informatique et des Libertés (CNIL) – however insists that the right to be forgotten should be respected beyond the territory of the European Union. Nevertheless, it is up to the CJEU to take a decision on this matter. If the CJEU rules in favour of an extraterritorial application, this might pose a difficulty for EU Member States and European courts to enforce the Google ruling outside their own jurisdiction.

A final decision from the ECJ is expected at the earliest in 2019.

Canadian Data Protection Authority issues annual report

On 21 September 2017, the Canadian Privacy Commissioner, Daniel Therrien issued an annual report to Parliament. The purpose of the report is to issue actions and recommendations with the aim to enhance privacy protection by introducing legislative amendments in order to counter current consent challenges. The report also covers the Commissioner's privacy work between April 2016 and March 2017 based on the Privacy Act and the Personal Information Protection and Electronic Documents Act.

Since the Commissioner states that “Canadians fear that they are losing their privacy” is a reality, they expect concrete, robust solutions to restore their confidence in technology as something that will serve their interests and not be a threat to their rights”. Therrien furthermore believes that “Canadians need to be supported by an independent regulator with the legislation and resources necessary to properly inform citizens, guide industry, hold businesses accountable, and sanction inappropriate conduct. Canadians do not feel protected by a law that has no teeth and businesses held to no more than non-binding recommendations.”

In that respect, Therrien states the need for, amongst others:

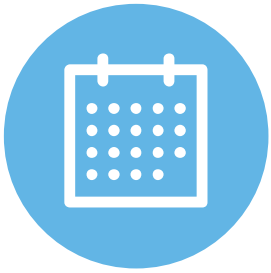
- Amending the current federal private sector privacy law to increase the Commissioner’s enforcement powers, including the power to issue orders and impose administrative monetary fines;
- Up-to-date guidance on how to obtain consent in an online environment, outlining four key elements that must be present in privacy notices and be explained in a user-friendly way;
- Guidance setting forth the areas in which the collection, use and disclosure of personal data is not allowed, such as in the event the processing of data would cause significant harm to the data subject;
- Modernising the Privacy Act for the public sector.

It remains unclear however how the Canadian Parliament and Government will respond to this annual report. A decision to amend the current legal framework could ultimately have an impact on its current adequacy status in relation to data transfers coming from and towards the European Union.

Enforcement

- ICO as well as the FTC are investigating Equifax, a US based credit reporting agency, that suffered a cyber security breach on 29 July 2017. Amongst others sensitive information, social security numbers, birthdays, addresses and credit card numbers of 143 million UK, Canadian and US customers were exposed in the breach. On the US side, senators are introducing a Data Broker and Transparency Act holding data brokers accountable for data breaches in the future.
- Spain has imposed a fine of EUR 1,2 million on Facebook for data harvesting activities, and failing to obtain users' express consent for processing sensitive personal data.
- True Telecom Ltd. a telecom company that was making illegal nuisance calls despite earlier warnings by the ICO, was fined £85,000.
- Cab Guru Limited, a company behind a taxi booking app has been imposed a fine of £45,000 by the ICO for sending out spam messages to customers without obtaining the necessary prior consent.
- Your Money Rights was fined £350,000 by the ICO for carrying out automated calls to customers during a period of 4 months in the absence of obtaining their specific consent.
- Whatsapp has been imposed a fine of EUR 3,000,000 by the Italian Antitrust Authority for forcing its users to consent to the sharing of their personal data with Facebook.

Conferences



European Privacy Academy

Deloitte Gateway Building, Brussels Airport, Belgium, 26 February – 1 March 2018
http://www.europeanprivacyacademy.com/

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

CPDP 2018

Brussels, Belgium, 24 – 26 January 2018
http://www.cpdpconferences.org/index.html

The Computers, Privacy and Data Protection conference is a three-day conference dedicated to privacy and data protection. This year, the overarching theme will be "the internet of bodies".

Data Privacy Day

28 January 2018

Data Privacy Day is dedicated to commemorate the signing of the Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data. Every year, on 28 January, public authorities and private organisations raise awareness on personal data protection and privacy. With the date of the GDPR approaching, this day will mark an interesting point in the step for GDPR compliance.