Privacy Flash – Issue 23

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

- California enacts new Privacy law
- Post-Brexit adequacy
- Privacy Shield
- Belgium publishes law implementing GDPR
- Italy's GDPR implementation law approved
- MEPs approve new data protection rules for EU Institutions
- First enforcement action under GDPR
- Big Brother Watch v. UK

News

California enacts new Privacy law

The California Consumer Privacy Act (CCPA) is due to come into effect in January 2020, with the potential of becoming the toughest and most important US law implemented in the privacy panorama.

Definition & Applicability

This law defines personal data as any information that "*identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.*"

The CCPA will apply to Californian residents ("consumers") and will be enforced against a business entity that collects or authorises another one to collect personal data on their behalf, AND that either:

- "*(A) Has annual gross revenues in excess of twenty-five million dollars [...];*
- *(B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices;*
- *(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information*".

Individual rights & transparency

Although the real impact of the new law is still unclear, the implications of the CCPA in terms of transparency and user control are yet appealing.

Following the path marked by the GDPR, the CCPA will introduce relevant changes to the processing and monetisation of personal data, empowering Californian residents with enhanced privacy rights.

Under the CCPA, consumers will be entitled to:

- **access their personal data**
- **request their personal data in readily transferable electronic format**
- **know what types of data a business entity has collected about them and ask for their deletion**
- **know whether their personal data is either sold or disclosed by a business entity** (consumers & minors or their parent/guardian must affirmatively authorise the sale of their personal data)
- **object to the sale of their personal information**
- **not being discriminated as to the service and price provided if they opt out of the sale of their personal information**. This however, does not prevent business entities from providing consumers monetary incentives and differentiated prices and services if "*reasonably related to the value provided to the consumer by the consumer's data*."

The CCPA also introduces the principle of transparency under which business entities must provide an updated privacy policy, informing consumers of:

- the categories of personal data collected
- the sources from which personal data is collected
- the purpose for which the personal data is collected
- their individual rights and how to exercise them
- the third parties with whom their personal data is shared
- the personal data that is collected, shared and sold to other parties

Private right of action

Finally, it is worth mentioning that the CCPA recognises Californian residents with a private right of action following "*an unauthorised access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information*".

The recovery of damages ranges between $100 to $750 per consumer per incident or actual damages, whichever is greater and requires the consumer to provide the business entity with a 30 day written notice to cure the incident and notify the Attorney General before initiating any action.

GDPR vs. CCAP

The table below compares their key elements[1]:

Element	GDPR	CCAP
Definition of personal data	"*Any information related to an identified or identifiable natural person*."	Information that "*identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*."
Who must comply?	Controllers & processors	Organizations that conduct business in California and meet one or more of the following requirements: • Annual revenue exceeds $25M • Buy or sell personal information about at least $50K individuals, devices or households annually • More than half of annual revenue comes from selling data about CA residents
Whose data is protected	Data subjects	"Consumer" means a natural person who is a California resident.

[1] A more comprehensive table can be found at: https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act.

Element	GDPR	CCAP
Fines	• up to €10 million or 2% of the company's global annual turnover of the previous financial year, whichever is higher. • up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher.	• Damages of up to $2,500 per violation for those violation(s) in which a Business Entity did not cure within the 30-day window; and/or • Damages of up to $7,500 per violation for those intentional violation(s) of the CCPA.
Key differences	The **GDPR**, but not the CCPA, covers the following elements: • Data Protection Officer (DPO) • Risk assessments • Data Protection Impact Assessment (DPIA) • Cross-border data transfer • Privacy by Design • Data retention • Right to not be subject to automated decision making	
Common elements	**Individual rights, Providing consent.**	

Coming up

These new compliance challenges may be subject to further modifications in order to clarify the many ambiguities they raise (e.g., The contrast within the principle of discrimination). There is however a risk that corporations may exert pressure to undermine the privacy rights of the consumers and dilute the data protection provided.

Post-Brexit adequacy

The uncertainty of the Brexit negotiations raises questions as to the potential impact on data flows between the UK and the EU.

In this scenario, there are several possible (more burdensome) outcomes under Articles 44-50 of the GDPR. The transfers of personal data could be permissible based on binding corporate rules, approved codes of conduct or certification mechanisms, approved contractual clauses and perhaps an EU-US Privacy Shield type of arrangement.

As a third country outside the European Economic Area (the UK has already anticipated that EEA membership is not contemplated), the UK's most promising option would be the adoption of an adequacy decision by the European Commission.

With an adequacy decision in place, data exchanges could occur without the necessity for additional safeguards the UK must show to ensure an adequate level of data protection, achieved through either domestic law or international commitments. The UK Data Protection Act 2018 aims at pursuing the implementation of a proper data protection framework, in line with the GDPR.

The main challenge lies in the fact that the procedure behind the adoption of an adequacy decision takes an average of 28 months and may therefore cause

serious disruptions to UK entities in terms of financial and security developments. Also, the decision may still be withdrawn or modified at any time upon request of the European Parliament and the Council.

What are the potential impediments to the adoption of an adequacy decision?

The UK's Investigatory Powers Act 2016, which was challenged by the EU's Court of Justice ruling in December of 2016 should be considered as a potential impediment. The ECJ found that the "*general and indiscriminate retention of all traffic and location data of all subscribed and registered users relating to all means of electronic communication*" is inconsistent with EU law and that access to retained data should be restricted solely to fighting serious crime. Another element that could come into play, is the fact that as a non-EU member state, the disputed EU-US Privacy Shield would no longer apply to the UK, enabling the possibility of less restricted data transfers.

Privacy Shield

Following the decision of the EU Court of Justice in the Schrems case in 2015, which served as the basis for the inadequacy of the EU-US Safe Harbour, the US has once again been called upon to grant European residents a higher level of data protection.

In September 2016, the European Commission had already recognised the adequacy of the new transatlantic data flows agreement, the US-EU Privacy Shield, but not without concerns. This lasted until June 2018, when the Civil Liberties MEPs adopted a motion calling upon the Commission to suspend the above mentioned deal if, by 1 September, the US did not take measures to ensure compliance with the European data protection standards. The debate on the Privacy Shield reached its peak following the Facebook and Cambridge Analytica scandals (both organisations were certified under the US-EU Privacy Shield).

With the potential suspension of the Privacy Shield and in absence of a US federal law setting out uniform standards, US companies aiming to do business with EU will have to face very high burdens in meeting the compliance requirements.

Belgium publishes law implementing GDPR

On 5 September 2018, the new Belgian Data Protection Law of 30 July 2018 was published in the Belgian Official Journal. The new act enters into force immediately upon publication.

The new Belgian Data Protection Law ("DPL") repeals the previous Data Protection Law of 8 December 1992 and further implements certain aspects of the General Data Protection Regulation. The new law addresses the following matters:

Territorial scope

The new Belgian law applies to any processing of personal data in the context of the activities of the establishment of a controller or a processor in Belgium, irrespective of whether the actual processing occurs in Belgium or not.

Children's consent

The new law sets 13 years as the age as of which children must provide consent for the use of an information service. For children under the age of 13, parental or guardian's consent must be obtained.

Special categories of personal data

The GDPR enables Member States to introduce further conditions in relation to the processing of special categories of personal data. The Belgian law makes use of that possibility by introducing additional requirements for the processing of genetic, biometric and health related data, such as: the obligation to establish a list of individuals who are entitled to access these data or the assurance that these individuals are bound by confidentiality obligations.

Restrictions on right of information and other rights of data subjects

Under the new Belgian DPL, data subjects rights can be restricted in the case of prevention and detection of criminal offences, protection of important objectives of general public interest and control, inspection or regulatory missions related to exercising public authority. In those cases, controllers do not have to inform data subjects of the processing of their personal data.

Processing and freedom of expression and information

The new law reconciles the right to protection of personal data with the right of freedom of expression and information by introducing restrictions on data subject rights including their right to be informed of any processing of their personal data, when personal data is processed for journalistic purposes, and for the purposes of academic, artistic or literary expression.

Cease and desist procedure

It is now possible for data subjects under Belgian law to seek a cease and desist order which allow them to bring a claim of infringement of data protection obligations before the Court of First Instance.

Sanctions and penalties

The new Belgian law provides for administrative and criminal sanctions in case of infringement of data protection obligations.

Italy's GDPR implementation law approved

On 8 August 2018, the Italian Council of Ministers approved Legislative Decree n. 101/2018. The Decree aims at aligning the Italian Privacy Code (Legislative Decree n. 196/2003) and several other national laws with the General Data Protection Regulation ("GDPR"). The Decree entered into force on 19 September 2018.

While the GDPR is directly applicable in all EU member states (i.e. there is no need to transpose it into national law), it does leave room for manoeuvring as it allows these states to deviate on certain critical points. The Italian legislator decided to use this liberty and introduced the following deviations:

- From the age of 14 years, children can validly consent to the processing of their personal data in relation to information society services, directly offered to them.
- In terms of the processing of particular special categories of "sensitive" data, namely genetic, biometric and health data, the Italian data protection authority – the "Garante –, will issue every two years provisions on safeguard measures. The list will include a wide range of measures ranging from data security to data minimisation, information and respect for the data subjects' rights.
- Persons who have an interest of their own or act to protect a deceased individual, may exercise data subject rights concerning data related to the deceased individual. However, certain limitations apply.
- In case of spontaneous job applications, employers who receive CVs may provide their respective privacy notice at the time of the first useful contact. In such case, consent of the applicant will not be required.

These are only several of the deviations which were introduced by the new Italian Legislative Decree. The Garante has already spread an ambiguous message stating that it will be "more" tolerant during the first months, but since it is obliged to issue fines, such tolerance cannot be unlimited.

MEPs approve new data protection rules for EU Institutions

On 13 September 2018, the EU Parliament approved stronger and tighter data protection rules for EU institutions, bodies and agencies.

The new regulation is replacing the current 45/2001 regulation. The aim of the new regulation is to align data protection rules for EU institutions with the GDPR and the proposed e-privacy rules. The scope of the regulation is to be extended in 2022 to Europol and the European Public Prosecutor's Office after the Commission's review.

With this new regulation, the European Data Protection Supervisor's (EDPS) role will be strengthened as it will be able to impose fines on EU institutions or bodies that infringe data protection obligations.

While these new rules have been approved by MEPs, the formal approval of the Council is still required. The new rules will enter into force 20 days after publication and become applicable immediately.

First enforcement action under GDPR

The Information Commissioner's Office in the UK has issued the first enforcement action under the GDPR and under the UK Data Protection Act 2018 to a Canadian firm, named AggregateIQ.

The enforcement action was served under section 149 of the Data Protection Act 2018 under the form of an **enforcement notice** and required AggregateIQ to "*cease processing any personal data of UK or EU citizens obtained from UK political*

organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes".

AggregateIQ is a firm that has provided UK political organisations in the past with personal data which were used in campaigns such as the Brexit referendum in 2016.

While the firm is not established in the EU, its activities fall under the territorial scope of the GDPR as the ICO considered that AIQ's processing of personal data relates to monitoring of data subjects' behaviour taking place within the EU and therefore must be considered subject to the GDPR. AIQ was found to be in breach of Articles 5(a) – 5 (c) and articles 6 of the GDPR, relating to the processing of personal data in such a way that individuals have not been made aware and for a purpose other than those defined in the above-mentioned articles.

The firm has decided to appeal the ICO's decision under section 162 (1)(c) of the DPA.

Big Brother Watch v. UK

The European Court of Human Rights recently ruled in Big Brother Watch and others v. United Kingdom that aspects of the UK's secret surveillance programs infringed Article 8 (right to respect for private life) and Article 10 (freedom of the press) of the European Convention of Human Rights.

The ECHR analysed three different types of surveillance: the bulk interception of communications, intelligence sharing, and the obtainment of communications data from communications service providers.

While UK governments do have some leeway in determining exactly what kind of surveillance program is needed to protect national security, the operation of such systems must meet certain minimum safeguards.

The European Court of Human Rights considered that the surveillance schemes overseeing bulk interception and the regime for obtaining communications data from communication service providers infringed Articles 8 and 10 due to insufficient independent oversight and inadequate safeguards. The Court stated however that the regime for intelligence sharing with foreign governments did not violate the rights to privacy or freedom of expression.

The Court thus extended the scope of protection of privacy beyond just the content of communications intercepted by the UK government. The Court believes that metadata such as IP addresses, file transfer logs, email headers, etc. should benefit from the same protection as the content of the communication.

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 3,800 employees in 11 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 480 million euros in the financial year 2017.

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 264,000 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 2017, DTTL's turnover reached over $38.8 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.

© 2018. 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.