Data Protection within the Digital Economy

Forthcoming EU General Data Protection Regulation

Roland Bastin
Partner
Governance,
Risk & Compliance
Deloitte

Irina Hedea
Director
Governance,
Risk & Compliance
Deloitte

Laureline Senequier
Senior Manager
Governance,
Risk & Compliance
Deloitte

Alexander Cespedes Arkush
Manager
Governance,
Risk & Compliance
Deloitte

Aurélia Schwander
Consultant
Governance,
Risk & Compliance
Deloitte

Introduction and context

In 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU, which are currently based on the EU Privacy Directive 95/46/EC.

Now, the EU is in the final negotiation phase of the reform. The completion of this reform is a policy priority for 2015. The objectives of this new set of rules are to give citizens more control over their personal data and to simplify the regulatory environment for businesses in EU. The data protection reform is a key enabler of the Digital Single Market, which the Commission has prioritized. The reform will allow European citizens and businesses to fully benefit from the Digital Economy[1].

As a result of the digital market evolution, personal data is increasingly collected and exchanged. But what happens to this data? Could it fall into the wrong hands? What rights do citizens have regarding their personal data? These questions are raised more often especially in the context of the current trends in data breaches and data leakage cases involving personal data. Despite the significant negative consequences associated with them, such incidents have unfortunately only increased in recent years.

In this context, a EU unified legislation on data protection, the proposed General Data Protection Regulation (GDPR), for replacing the current patchwork of rules on the protection of personal data in the EU (harmonized by the EU Privacy Directive 95/46/EC), has become crucial for ensuring that the fundamental rights of citizens regarding their personal data are protected while sustaining the development of the Digital Economy.

What is personal data?

In the EU, "personal data" means any information relating to an identified or identifiable natural person ("data subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

There are different ways in which an individual can be considered "identifiable." A person's full name is an obvious likely identifier. But a person can also be identifiable from other information, including a combination of identification elements such as physical characteristics, pseudonyms, occupation, address, credit card number, bank statements, criminal record, etc.

When may the General Data Protection Regulation (GDPR) be expected?

The European Commission published its GDPR proposal in 2012. The European Parliament adopted its position in March 2014. On 11 June 2015, the Council reached a general approach on the GDPR[2]. The "Trilogue" i.e. the final negotiation between representatives of the Council, the European Commission, and the European Parliament commenced in June 2015 and is scheduled to end in December 2015. The final text is scheduled to be ready by the beginning of 2016 and clearer compliance goals could be anticipated for early 2018, when the GDPR is scheduled to come into effect. Considering the negotiations are still ongoing, this timeline might still change and the statements in this article are also subject to change.

1 http://ec.europa.eu/justice/data-protection

2 The EDPS has published a comparative view: https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/Consultation/Reform_package

"The data protection reform is a key building block of the Digital Single Market, and it brings benefits to citizens and business." Vera Jourová Commissioner for Justice, Consumers and Gender Equality[3]

What is the aim of the GDPR?

One aim of the GDPR is to facilitate economic growth. According to some estimates[4], the value of EU citizens' personal data could grow to €1 trillion annually by 2020. Strengthening Europe's high standards of data protection therefore means business—not a burden to innovation.

The Regulation will establish a single, EU-wide law for data protection, replacing the current inconsistent patchwork of national laws and thus enabling companies to deal with one law instead of 28. Furthermore, in certain international cases, organizations will deal with one supervisory authority instead of 28, rendering doing business in the EU simpler and cheaper. Also, certain rules pertaining to international data transfers, such as the approval of binding corporate rules, will be simplified.

Additionally, companies established outside of the EU targeting EU residents will have to apply the same data protection rules as those inside the EU.

Another aim of the GDPR is to ensure a high level of protection for EU citizens by creating trust in the digital market. It will empower citizens with a set of rights enabling them to be informed and remain in control of the use made of their personal data.

To this end, the GDPR introduces extensions of existing rights of individuals such as the right to be forgotten. It also brings novelties such as the right to data portability to allow individuals to have more control over personal data by transferring it more easily from one service provider to another.

What are the main features of the GDPR?

The new principle of accountability entails the responsibility for entities processing personal data to ensure compliance with the data protection principles described in the GDPR. It will require them to put in place controls and to document them. As a result, organizations will need to be able to demonstrate their compliance with the GDPR to national Data Protection Authorities (DPA), such as the CNPD[5].

Furthermore, the GDPR underlines concepts such as:

Privacy Impact Assessment (PIA)

In case the risk analysis of activities indicate a high risk (e.g. for activities such as the monitoring and profiling individuals or the processing of sensitive data such as health data), organizations will have to conduct a Privacy Impact Assessment (PIA). PIA is a tool for identifying and reducing the privacy risks but also for helping to design more efficient and effective processes for handling personal data.

Privacy by Design and Default

There will be an obligation to implement 'Privacy by Design' mechanisms when setting up new business processes. The European Parliament proposal states that Privacy by Design must take the entire lifecycle of personal data into account and should focus on safeguards that protect the accuracy, confidentiality, integrity, physical security, and deletion of personal data. In addition, there will be an obligation to implement privacy-friendly default settings which are referred to as "Privacy by Default."

3 *Remarks by Commissioner Jourová after the launch of the Data protection regulation trilogue: http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm*

4 *The EU Data Protection Reform and Big Data – Factsheet*

5 *http://www.cnpd.public.lu/*

Data Protection Officer (DPO)

The mandatory appointment of a Data Protection Officer (DPO), an internal function to oversee compliance with the GDPR, is still under debate. The Commission requires it of organizations with more than 250 employees; the European Parliament ties the appointment to the level of risk entailed by the processing; and the Council's proposal leaves EU Member States free to impose the designation of a data protection officer in their national law.

Transparency

Much emphasis is put on the principle of transparency that requires information relating to the processing of personal data (e.g. privacy statement) to be easily accessible and easy to understand, explained in clear and plain language. Therefore, organizations will have to explain in an understandable way and free of charge which user data they process in which context. This means that generic and legalese privacy statements will not suffice, more detailed information will be requested.

Consent

The GDPR will make the conditions for consent clearer. If the personal data processing is not necessary (e.g. due to a legal obligation or contract), organizations will need to obtain genuine consent from individuals. "Consent" still means any freely given specific, informed indication of an individual's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to the processing of his or her personal data. It will no longer be possible to integrate consent for secondary purposes into general terms and conditions.

Consent can be withdrawn freely at any time. Therefore, organizations will have to draft their consent forms carefully as well as reconsider the ways consent will be requested from citizens and clients especially since they will bear the burden of proof.

Data breach notification

Organizations will have to notify certain personal data breaches to the national DPA. The reporting will likely have to be done within 72 hours after becoming aware of the breach.

The duty of notifying certain data breaches is not limited to the DPA. Organizations will be obliged, in some situations, also to notify the individuals concerned by the data breach, unless appropriate security measures (such as encryption) are in place.

Of the boards that discuss technology IT risks, those most often covered include data privacy, which is discussed by 57 percent of the boards, and cybersecurity, which is discussed by 51 percent of them

How will the GDPR be enforced?

Supervisory authorities

The GDPR defines the concept of Data Protection Authorities for supervising the respect of data protection.

Whenever a case relates to multiple jurisdictions (e.g. data controller has establishments in many countries), the Data Protection Authority of the organization's main establishment will assume the lead, coordinate with other DPAs, take into account their opinions, and attempt to reach a consensus. However, the local DPA will remain the sole enforcement authority in its own jurisdiction.

Redress

Persons who have suffered (non-monetary) damage such as reputational or emotional damages will have the right to claim compensation from the controller or the processor for the damage. Prejudiced parties will be able to join forces through class action suits, even in countries where currently this is not possible.

Administrative sanctions

In the event of data protection violations, all DPAs in the EU will be able to issue a written (public) warning against infringers, subject them to regular audits, and impose administrative fines. The maximum fines are still under negotiation, but considering that the Commission and Council propose a maximum fine of up to €1 million or 2 percent of the annual worldwide turnover, and the Parliament proposes €100 million or 5 percent, organizations will have to update the risk rating for privacy compliance.

How should CIOs prepare for the forthcoming regulation?

Data privacy seems to keep CIOs awake at night. Of the boards that discuss technology IT risks, those most often covered include data privacy, which is discussed by 57 percent of the boards, and cybersecurity, which is discussed by 51 percent of them. In addition, data warehousing is discussed by 38 percent and international data transfer by 21 percent of the boards[6].

Given the restrictive nature of obligations introduced by the GDPR and the mass of personal data currently being processed and used by companies, it is clear that the proposed regulatory changes will have a profound impact on the operational, IT, and control environment of organizations.

Therefore, organizations should prepare by performing a maturity assessment as soon as possible to qualify their current situation against the one requested in the proposed GDPR. In addition, organizations should invest in quick wins by focusing on concepts contained in the forthcoming legislation (transparency, consent, the rights of access, etc.) to already start enhancing compliance.

6 *Information summarized from "Director 360°: Growth from all Directions", third edition: http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-director-360-growth-from-all-directions-third-edition.pdf*

In practice, CIOs should prepare by taking care that an overview exists of the personal data and IT systems processing that data. An IT architecture hosting the organization's personal data that is clearly identified and documented will ease the implementation of the data protection governance through the whole data life cycle. CIOs should support data protection by implementing the required information security measures in the IT environment hosting personal data. Data protection should be part of IT project management processes but also of the incident management processes for allowing the identification and notification of data breaches.

Additionally, it is key to coordinate with the business owners for updating existing documentation such as policies, procedures, privacy notices, and consent forms before implementing tools such as a Privacy Impact Assessment or Privacy by Design and Default to get set for the future.

Today the GDPR is not yet final—changes might still come. Nevertheless, the organizations already starting preparing themselves to be ready when the Regulation comes into effect will have a competitive advantage in the Digital Single Market and will be prepared for meeting the regulatory requirements.

New updates will be provided when the final text of the GDPR is known.