Deloitte.

EU agrees on new Privacy Regulation

Changing the privacy landscape for businesses

January 2016

On Tuesday 15 December 2015, the European institutions agreed on a final text for the new General Data Protection Regulation (GDPR). The GDPR - proposed by the European Commission in 2012 – will replace the former EU Data Protection Directive and create a unified data protection law that will apply directly across all 28 EU Member States from 2018.

Changing the privacy landscape for businesses

With the new Regulation, the EU intends to strengthen citizens' control over the use of their personal data, while simplifying the regulatory landscape for business. An **integrated mechanism** will allow individuals to make complaints about the misuse of their data with the Data Protection Authority (DPA) in their home country, rather than where the company is based. Individuals will also be able to join in class action suits through representative organisations (such as consumer protection organisations), who if allowed by national law, may also act on their own initiative.

Companies will be obliged to **notify data breaches** to the competent supervisory authority without undue delay and not later than 72 hours after discovering it. One way to avoid infringements is to implement appropriate technical measures (e.g. pseudonymisation) prior and at the time of processing to ensure compliance with data protection principles (**Privacy by Design**, described below). In the event of non-compliance with the law or infringements of individuals' rights, **companies can expect administrative fines of up to 20 million euro or 4% of their total global annual revenue**. All DPAs will get the power to issue such enforcement actions, either directly or through national courts.

Public authorities and bodies that process personal data; organisations whose core activities require regular and systematic large-scale monitoring of individuals; and organisations where large-scale sensitive personal data processing takes place, will now have to appoint a **Data Protection Officer (DPO)**. In addition, national law may require other organisations to appoint a DPO. A DPO's main tasks will consist of monitoring compliance with the privacy principles set by the GDPR, and managing the relationship with both data subjects (employees, customers) and the supervisory authorities.

To ensure that privacy is taken into account throughout the business and at the start of each new process or project that involves the use of personal data, the GDPR introduces the concept of **Privacy by Design**. To ensure that this principle is implemented, the Regulation obliges organisations to carry out **Data Protection Impact Assessments (DPIAs)** before the processing starts, if the processing is considered high-risk for the rights of individuals.

Aside from reaffirming core privacy principles such as purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality; the Regulation shifts the regulators' focus towards **accountability**. This implies that the data controller shall be responsible for, and be able to demonstrate, compliance with the Regulation. Privacy and information security policies and procedures, personal data processing records (such as inventories or data flow mapping), documented training and awareness programmes, Data Protection Impact Assessments and compliance/audit plans will be considered key elements in this respect.

Strengthening citizen's fundamental rights

One of the main raisons d'être for the new Regulation is the EU's aim to restore consumers' trust in how data is processed in an online environment. The law therefore reaffirms that citizens have a **right to be forgotten**, which will require businesses to erase personal data when requested to do so, provided certain conditions are met. In the event a business offers online services (e.g. e-commerce, social media) to a child, the **age of valid consent** has been set at 16. Individual Member States can however lower this age in their jurisdiction, to as low as 13.

Member State law may still create differences

While the GDPR is intended to streamline data protection laws in the European Union, a complete harmonisation has not been established. The Regulation allows the Member States to go beyond the Regulation in several areas, including to determine in which additional circumstances a DPO

must be appointed. DPOs and other privacy compliance officers should therefore continue to monitor changes to national privacy legislation in the Member States as well.

What's next?

While negotiators of the European Council and the European Parliament reached an agreement on the final text of the Regulation, both institutions still have to formally adopt it. The responsible Parliament Committee has passed the GDPR with 48 votes for and 4 against on 17 December 2015, which means the Regulation will be presented to the full plenary session of the Parliament in the first months of 2016. In addition, the heads of state of the EU Member States are scheduled to meet in February 2016, and are likely to vote on the Regulation then.

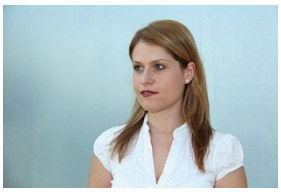
As soon as both the Parliament and the Council have formally adopted the text and the GDPR is published, a two-year period will commence in which organisations and regulators will have the time to prepare for the formal entry into force of the Regulation in Q2 2018.

Date	Legislative step
18-19 February 2016	European Council expected to formally adopt the GDPR
March - April 2016	European Parliament plenary expected to formally adopt the GDPR
Q2 2016	Expected publication of the GDPR in the Official Journal of the European Communities
Q2 2018	Formal entry into force of General Data Protection Regulation

Contact

Roland Bastin
Partner - Information & technology Risk
rbastin@deloitte.lu

Laurent de la Vaissière
Director - Information & Technology Risk
ldelavaissiere@deloitte.lu



Irina Hedea
Director – Information & Technology Risk
ighedea@deloitte.lu