Deloitte.

Belgium | Deloitte Enterprise Risk Services | 18 November 2015

General Data Protection Regulation
A summary

The General Data Protection Regulation (GDPR) will supersede all current national data protection laws in the EU. The European Commission published its proposal in 2012, with the European Parliament adopting its position in March 2014, and the Council of the European Union adopting its view in June 2015. Since June 2015 the 'trilogue' negotiations between the three institutions have been taking place and are scheduled to complete in December 2015. This implies that we should know the final text of the GDPR at the beginning of 2016, allowing organisations to set clear compliance goals in advance of it coming into force, after a two year transition period, in early 2018.

Overview

Although the GDPR is not yet finalised, here is an overview of the main expected changes that organisations will have to be aware of and adapt to:

Regulation

- Harmonisation of national data protection law across the EU
- Single set of principles and rules across the EU (fewer conflicting obligations, making it theoretically easier to do business across the EU)
- Directly applicable across the EU without the need for national implementation

Data Protection Officer (DPO) – Appointment within a company

- Not mandatory under the Council's approach, leaves the decision to the Member States
- Compulsory according to the Commission's proposal where companies have 250+ employees or when personal data processing represents a high risk for individuals
- Compulsory according to Parliament's amendment: DPO employment obligatory for data processing of > 5000 individuals, or when personal data processing represents a high risk for individuals

Enforcement

- The likelihood of enforcement influences a business's approach to compliance
- More and uniform enforcement powers to the relevant data protection authority e.g. GDPR breach investigations, enforcement action in case of a breach, main forum of complaints for the individuals
- In international cases, a single data protection authority will be the lead supervisory authority, based on where the organisation's main EU establishment is ('one stop shop')
- Substantive administrative sanctions/penalties (EUR 1-100 million/2-5% of annual worldwide turnover)

Accountability

- Organisations must implement policies and procedures to ensure compliance with the Regulation (codes of conduct, certifications)
- Registration of data controllers and their processing to the data protection authority will be abolished (likely to be replaced by an obligation to maintain internal records of personal data processing operations for organisations with 250+ employees)

Right to be forgotten

- Obligation to erase personal data without undue delay where the data is no longer needed for original purpose, data subject has withdrawn its consent, data was unlawfully processed, data subject objects (impact on data transferred to third parties: to be decided)

Data portability

- Right for individuals to obtain their data in a reusable format and transfer it to another service provider
- Encouragement of organisations to work towards interoperability as regards data and its format

Privacy by design

- Businesses need to take privacy and data protection issues into account from the start of any product design process and properly assess the risks before launching any new products
- Whenever a business develops or designs a new technology, product or service, it should do so in a way that ensures compliance with data protection obligations

Privacy impact assessment

- Businesses need to conduct Privacy Impact Assessments (PIAs) as a mechanism to assess privacy risks, identify measures to address these risks and demonstrate compliance with the GDPR (identification of the maturity level of your company)

International data transfers

- Restrictions on the transfer of personal data outside the EU (and the permitted pathways e.g. Binding Corporate Rules, Model Contract Clauses) remain
- The European Court of Justice ruled on 6 October 2015 that the Safe Harbor Framework for transferring personal data from the EU to the US was invalid. The European Commission published guidance on 6 November 2015 which confirmed the above and stated that its objective is to conclude negotiations with the US on a new framework to replace Safe Harbor within 3 months (Recommended reading: Navigating the Safe Harbor Storm). Please check with us for the latest updates on this.

Data breach reporting

- Each data breach should be reported to the relevant data protection authority within 24 or 72 hours, when feasible (this time period has yet to be decided)

What can your company do to prepare for the new regulation?

- Establish comprehensive policies and procedures and get director/board sign-off where appropriate, to ensure all privacy requirements are documented and reviewed
- Encrypt as much of your personal and business confidential data as is practicable and on a risk-based approach, paying particular attention to sensitive personal data, mobile devices and data transfers outside the business
- Assess and minimise risks by conducting privacy impact assessments on data processing and the supporting IT systems
- Document and raise awareness of what to do in the event of a data breach – reporting of these will need to happen in a tight timeframe and companies will have to document what has been lost, how the leak was addressed etc.
- Document decision processes, conclusions and breaches thoroughly – the relevant data protection authority may request this and base any possible sanction on how well prepared you were
- Make extra effort to be transparent to customers, explaining clearly and simply how personal data is handled
- Keep a comprehensive record of consent given - proof of will have to be presented on request to the relevant data protection authority. The burden of proof is on the company.
- Make sure all relevant staff receive training in data protection so they know what they need to do or when they need to ask questions. Proof of training is also important in cases of negligence or malicious actions.
- If your company has more than 250 employees, or processes more than 5000 people's data, consider who should be your Data Protection Officer and formalise this role.

How Deloitte can assist you

Deloitte offers a range of data protection and privacy-related services and can help you adapt to the measures outlined above.

Deloitte is also able to assist your company in providing department-specific privacy training and assist on leveraging existing PIA tools.

Examples of our services include Privacy Impact Assessments, inventories and mapping of personal data processing, privacy compliance quick scans, ad hoc privacy helpdesk services and more.

Our services allow you to make maximum use of the data within your databases and systems, in full confidence that you are in compliance with privacy and data protection regulations. To find out more please click here.

For further information, please contact:

Erik Luysterborg
Partner
BE Security & Privacy Leader
EMEA Data Protection & Privacy Leader
eluysterborg@deloitte.com

Homepage

Deloitte Belgium
Berkenlaan 8A, 8B, 8C
1831 Diegem
Belgium