Why to check now if your business is prepared for the coming EU General Data Protection Regulation

The EXIN blog takes a look at the coming EU General Data Protection Regulation (GDPR) and the major impact it is going to have on businesses and organizations globally.

What is the GDPR

The European Union General Data Protection Regulation is the new set of rules that will replace the current Data Protection Directive. It will apply in all member states from 25 May 2018 without having to be transposed into national law first. The European Commission asserts that the reform will facilitate business in the Digital Single Market. This will be achieved by doing away with costly administrative burdens that arise from the current fragmentation of rules in the different countries. For companies, the harmonisation of the rules has the potential to require large-scale adjustments in the way they deal with personal data. Not just in the EU.

Main characteristic: Its wide reach

The scope of the regulation is quite extensive. It covers far more companies than those in the member states of the EU. Any organization in the world that offers goods or services to EU residents OR monitors the behavior of EU residents will be subject to its rules. In addition, both personal data and data breaches are defined rather broadly: The regulation considers personal data to be “any information relating to an identified or identifiable natural person.” A data breach refers to any “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

Beyond these definitions, the new regulation is governed by a few broad data protection principles: It aims to ensure that data is only collected for legitimate purposes, that only data needed for those purposes is stored, that it is fairly and lawfully processed and that the data isn’t held for longer than necessary. With businesses collecting and analysing increasing amounts of information on consumer behavior and internet habits, the GDPR is the EU’s answer to the increasing risks of cyber crime (read more about this topic here).

With only one year remaining until the regulation enters into force, companies are best advised to check if their employees are up to date on the new changes. Next, we will take a look at the most important ones.

New rules with operational implications

The existing data protection rules will undergo major changes in a few key areas. These will have wide ranging implications for organizations.

Privacy by design and by default

Data protection must not only be a key consideration for companies. They will have to be designed into the planning and implementation of new products and services which affect personal data. By default, privacy settings must be set to a high level. The GDPR even spells out, which security actions it considers appropriate to meet its requirements and to ensure accountability. The regulation further specifies, which code of conduct and which certification mechanisms are recognized for controllers to prove compliance with its security standards.

72-hour breach notification

In the event of a personal data breach, the data controllers of an organization have to act quickly. They are required to report the breach to the supervisory authority no later than 72 hours after having become aware of it. Should the controller find that the breach is likely to pose a high risk to the rights and freedoms of individuals, the affected persons must be informed immediately.

Consent

Obtaining valid consent from people becomes more complex. Consent has to be given freely, be specific to the purpose for which the data is used and the user has to be properly informed about the purpose as well as the right to withdraw consent. In case of sensitive data or transborder data flow, it must be explicit stated and controllers have to be able to provide evidence of consent.

Rights of data subjects

Under the new GDPR, individuals are gaining a number of rights:

Right to rectification — Anyone will be able to gain access to their personal data and can have it corrected.

Right to restriction of processing — Under certain circumstances, people will be able to request a restriction of processing of their data.

Right to data portability — Users can ask for the data they have provided to an organization or social media platform. They also gain the right to transfer their data to another provider without hindrance.

Right to be forgotten — This right allows people to request that any data relating to them is erased without undue delay. They can make such a request on various grounds including withdrawal of consent and unlawful processing.

Right to object — Consumers have the right to object at any time to the processing of their personal data. This includes profiling.

Sanctions

One important new feature of the new regulation is its dramatically increased scope for sanctions in case of non-compliance. For a single breach, the European Commission will be able to fine an organization a maximum of €20 million or 4% of annual worldwide turnover, whichever the greater sum.

Transitional period

The new regulation has come into effect on 24 May 2016 and its application will commence on 25 May 2018. Thus, the European Commission grants organizations a two year transitional period to get ready to comply with all of the rules. One year is left to

How to prepare for the GDPR

If your business has not yet taken action, here are a few key questions that you should ask yourself:

- Do you have a data protection program?
- Can you provide evidence of how you comply with the requirements of the EU GDPR?
- Are you able to notify the new supervisory authority of a data breach within 72 hours?
- Do you design data protection and privacy requirements into the development of your business processes and new systems?
- Do you know how you will comply with the ‘right to be forgotten’, the ‘right to data portability’ and the ‘right to object to profiling’?

Organizations unsure about how to deal with these daunting challenges would be advised to first take a close look at the competences of their employees dealing with information and communication technology (ICT). The regulation explicitly spells out obligations of data controllers and data processors. Thus, data processors are added to the list of officially regulated entities. As the financial ramifications of breaching the broadened rules can be severe, investment in qualified personnel is the best path to ensure a smooth transition.

Get certified

EXIN offers a range of globally accepted certifications that ensure that your ICT professionals fully comply with all data protection regulations. As part of the Cyber Security and Governance Portfolio, EXIN evaluates candidates' skills and competences in the following fields:

Privacy and Data Protection - At the end of this certification, ICT professionals are well prepared for implementing the EU GDPR as well as the EU-US Privacy Shield Framework.

Secure Programming - This module certifies that candidates know how to build secure systems and software. A particular emphasis lies on preventive measures during the development phase of a product or service. These should be a key component of an organization's security considerations.

Ethical Hacking - This certification provides proof that the ICT professional knows how to test software and web applications for vulnerabilities by using the same methods applied by hackers. Having competent personnel in this area will allow you to test the resilience of your system and assess the likelihood of data breaches.

1082 words

Tags: General Data Protection Regulation, GDPR, EU, EC, European Commission, regulation, harmonization, data protection, privacy, breach notification, breach, personal data, right to be forgotten, right to data portability, data portability, restriction, processing, profiling, privacy by design, privacy by default, consent, secure programming, ethical hacking

For Twitter/LinkedIn:

How prepared is your organization for the new #EU General #Data #Protection Regulation? Join the #Exin blog on #GDPR <InsertLink23Character>