PECB

When Recognition Matters

PREPARING FOR COMPLIANCE WITH THE GDPR

The aim of General Data Protection Regulation (GDPR) is to create a uniform level of data protection in the European Union (EU). Before the EU data protection becomes enforceable, it is crucial for organizations to ensure their compliance with the GDPR requirements. This new regulation will apply to all organizations that process personal data of the EU citizens and will allow them to continuously monitor personal data breaches. The General Data Protection Regulation will enter into force on May 2018 and will replace the Data Protection Act (Directive 95/46/EC). Even though that GDPR and Data Protection Act (DPA) have many similarities, there are still significant changes. With this new regulation, the shape of future data protection's framework in EU is clear.

Subject to the GDPR won't be only the companies in the EU, but also the companies outside of EU which are targeting consumers in the EU. In case organizations fail to comply with the GDPR requirements, the penalties can reach up to 2% of an organization's annual turnover. Also, in the case of more serious infringements, the penalties can amount to 4% of an organization's annual revenue. Under certain circumstances, the GDPR obliges the organizations to appoint a Data Protection Officer (DPO). The DPO may be employed or work only under a service contract.

THE DIFFERENCE BETWEEN THE DATA PROTECTION ACT (DPA) AND GDPR

Currently, the UK relies on the Data Protection Act legislated in 1998, effective after the withdrawal of the EU Data Protection Directive 1995. The Data Protection Act will be automatically replaced with the enforcement of GDPR.

Scope

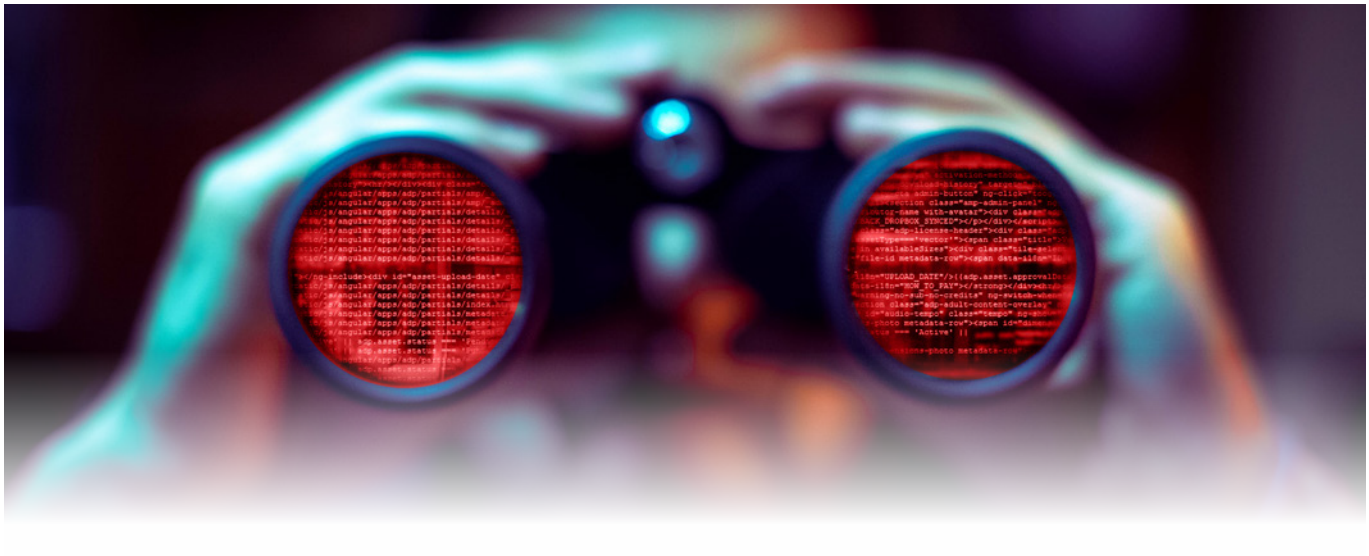
The Data Protection Act applies only to those in the UK, while GDPR applies to any organization that holds or processes EU citizens` personal data, without taking into consideration if the company is based in the EU or not.

Opt-In

The Data Protection Act requires a negative-opt, whereas with GDPR in place, organizations will be allowed to send e-mails only to people who have opted-in to receive messages.

Fines

In case of serious breaches, the Data Protection Act carries fines up to €500K, whereas with GDPR, the fines for serious breaches can be up to €20 million. Such fines could result in the closure of many businesses.



Personal Data Requests

Under the Data Protection Act, organizations were allowed to charge a reasonable fee for data requests, and the rights for erasure were a matter of common law, whereas under GDPR these are free, and data subjects have the explicit right to ask for data erasure.

Breach Reporting

Under the Data Protection Act, the reporting of data breaches was required only if the breach was also covered by the Privacy and Electronic Communications Regulations 2011, however, under the GDPR, reporting a data breach is mandatory in cases when breaches put at risk the freedom and rights of the individual.

STEPS TO GET PREPARED FOR GDPR

1. Raise awareness

Ensure that organization`s key people and decision makers understand the impact of GDPR implementation and are able to identify areas that might cause problems during this process.

2. Accountability and Data Governance

Documentation of what personal data is held, what is the source of this data and with whom the data is shared. In addition, it may also be necessary to conduct an information audit within the organization.

3. Communicate privacy information

Review the current privacy notices and create a strategy for making any required changes in time for GDPR implementation.

4. Individual's rights

Procedures should be checked to ensure that they contain all the individuals` rights, including the methods used by the company to delete personal data or provide data in an electronic form or an acceptable format.

5. Subject access requests

Update procedures, and set a plan on how to handle requests within the new timescales and provide any additional information.

6. Legal basis for processing personal data

Based on the types of data processing carried out, a company should identify and document the legal basis for processing personal data.

7. Consent

Review on how the consent is sought, recorded and managed and whether any changes need to be made.

8. Children

When performing data processing activities, consider setting systems for verifying the age of the individuals and gathering consent from parents or legal guardians, if needed.

9. Data breaches

Development of the right procedures and policies used to detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments

Familiarization with the ICO guidance on Privacy Impact Assessments and determine how and when they should be implemented in the organization.

11. Data Protection Officers

To ensure data protection compliance in an organization, it may be necessary to appoint as Data Protection Officer someone from the organization or an external data protection advisor.

12. International

If the organization operates internationally, it should define which data protection supervisory authority will be accountable for its regulation.

In conclusion, all organizations must be aware of the GDPR requirements and be prepared to comply by May 2018. They should consider this as an opportunity, thus, when preparing for compliance, organizations need to go beyond data protection and embrace data control and transparency. By doing so, businesses will have significant benefits from avoiding costly punishments, while improving customer data protection and trust.

Author: **Endrita Muhaxheri** is the Portfolio Marketing Manager for Governance, Risk, and Compliance & Health, Safety and Environment at PECB. She is responsible for continually conducting market research and writing articles and marketing materials related to GRC and HSE. If you have any questions, please do not hesitate to contact her: marketing.rm@pecb.com.