GLOSSARY

The new EU personal data regulations

– The concepts you need to know

eBoks

Are you up to date with the new EU personal data regulations? Here are the concepts you need to know to be fully prepared for 25 May 2018, when the new regulations come into force.

Here we have collected a list of the most important concepts you need to know to be well-prepared for the when the law comes into force on 25 of May 2018.

Accountability
The data controller needs to document that the company complies with the new regulation's privacy principles and requirements.

Consent
Data subjects must give permission for the processing of their personal data. This consent must be voluntary, specific and informed. The company needs to provide information on which personal data is collected, for what purpose, and who will process this data. There are special rules for how data is collected with regard to the personal data of children.

DPIA (Data Protection Impact Assessment)
The data controller needs to conduct a risk analysis to ensure that all personal data in the organisation's IT systems is adequately protected. If a risk analysis shows that the processing of data has a high risk in relation to the rights of the data subject, a DPIA must be conducted. The reason for conducting a DPIA is to give an overview of the consequences of processing personal data within the organisation, and to explore the possibility of improving procedures for processing.

Data breach notification
The data controller has an obligation to notify the relevant authority in cases of data breach within 72 hours. In Denmark, the national data authority is the Datatilsynet. The notification must include a description of the data breach, contact information of the DPO (or another contact person in the organisation), a description of any possible consequences of the data breach, and a description of the organisation's action plan in connection with the data breach.

Data controller
The entity responsible for the organisation's processing of data. The data controller decides how and for what purpose the personal data is processed. The organisations themselves are typically the data controllers of their own customer and personal data.

Data processor
The entity processing the personal data (on behalf of the data controller). The data processor may be an external contractor responsible for the organisation's IT systems. Examples of data processors in organisations include third parties that host the organisation's mail server, finance program, customer database and similar.

Data Protection Officer (DPO)
Many companies need to have a person responsible for data protection. This, however, does not apply to small and medium-sized enterprises unless the main/core activity of these organisations is data processing. The DPO must be independent, and is also responsible for informing and consulting the data controller, data processor, and the employees processing personal data about their obligations regarding the new regulations. The DPO functions as a contact person for the Datatilsynet (Denmark's national data authority) or equivalent European authorities.

Data subjects
The person the data concerns.

Digital Single Market
The new personal data regulations are part of the EU strategy; Digital Single Market, which is intended to harmonise the EU member countries' digital market.

European Data Protection Board
The board responsible for monitoring and advising on GDPR issues.

GDPR
General Data Protection Regulation.

Information notice
Companies must always inform data subjects about the purpose of the data collection.

Personal data
All information or data that directly or indirectly can identify a particular individual

Privacy by design
A principle designed to ensure that personal data is protected throughout the flow of information in an organisation's IT systems and processes. The principle is the technology-based design approach used to ensure that the rights of the data subject are protected when individuals and organisations, for example, develop or make use of devices, software and apps.

Privacy by default
A principle which means that organisations must provide data subjects with a default level of high personal data protection. In addition, the principle must prevent collection, display or forwarding of personal data which is not included in the data subject's consent.

Right to data portability
The data subject has the right to obtain their own personal data, and also to transfer the data to another data processor.

Right to be forgotten
The data subject has the right:

1. to be forgotten
2. to deletion in the organisation's system
3. to withdraw consent.

Territorial Scope
GDPR applies to the processing of all data in the EU, as well as for organisations outside the EU that supply goods or services to EU citizens. This territorial extension means that many non-EU organisations will also have to comply with GDPR.