

EU General Data Protection Regulation (GDPR)



GENERAL INFORMATION

The EU General Data Protection Regulation (GDPR) replaces Data Protection Directive 95/46/EC of 1995. The GDPR applies to the whole of the European Union. It prohibits the use of personal data unless authorised by another regulation. This means that anything not expressly permitted in the regulation is considered to be prohibited.

- ▶ The content was agreed by the European Council, the European Parliament and the European Commission on 15.12.15
- ▶ The regulation was adopted on 14.04.16 by the European Parliament
- ▶ It cannot be made more or less stringent by national laws
- ▶ It has flexibility clauses allowing certain issues to be regulated at national level
- ▶ It is focused on personal data



FROM

25.05.18

THE GDPR WILL APPLY TO ALL EU MEMBER STATES

OBJECTIVES OF THE REGULATION

UNIFICATION

Uniform data protection legislation throughout Europe



MODERNISATION

Modernise data protection law, especially with regard to globalisation and increasing digitalisation

STRENGTHEN RIGHTS

Strengthen and clarify the rights of those concerned in the EU



DELETION

Right of deletion (the 'right to be forgotten')

SIMPLIFICATION

Simplify processes and requirements for all countries that interact with more than one EU State



MOVEMENT OF DATA

Free movement of data within the European Single Market

PRINCIPLES

7

SEVEN PRINCIPLES OF DATA PROTECTION LAW

THE EXISTING HAVE BEEN RETAINED



- ▶ Lawfulness, good faith, transparency
- ▶ Purpose limitation
- ▶ Adequate, relevant and not excessive
- ▶ Accuracy
- ▶ Storage limitation
- ▶ Integrity
- ▶ Confidentiality

BUSINESS REQUIREMENTS

SCOPE

Applicable to companies that process personal data in the EU



PENALTIES

Fines of up to €20 million or 4% of the previous year's turnover



COMPULSORY NOTIFICATION

Notification requirement in the event of data loss or security breaches: max. 72 hours. Otherwise fines of up to €10 million or 2% of the previous year's turnover.



ROUTINE MEASURES

Regular audits, data protection documentation, data security measures and risk analyses



DEADLINES

Short deadlines for regulation and corrective action

AUTHORITIES



EUROPEAN DATA PROTECTION BOARD

EU-wide



SUPERVISORY AUTHORITY

National level



DATA PROTECTION OFFICER*

Company level

THERE ARE

3

AUTHORITIES RESPONSIBLE FOR THE IMPLEMENTATION OF THE GDPR

*To be appointed by any EU company if it processes the data of more than 5,000 people a year.