EU Data Protection—GDPR

The General Data Protection Regulation

Since May 25, 2018, the new EU General Data Protection Regulation (GDPR) applies in all EU member states. Increased obligations on data controllers and processors, and extended rights for data subjects, mean that businesses will have had to make significant changes to their data protection practices to ensure that their processes, policies and contracts conform to the GDPR.

Scope

The GDPR applies to data controllers and processors established in the EU, whether or not the processing actually takes place in the EU, and also to data controllers and processors who are not established in the EU, if the personal data processed concerns data subjects in the EU and the processing relates to offering them goods or services or monitoring their behavior.

Rights and Obligations

Accountability is a key principle under the GDPR: companies not only have to comply with the GDPR but also have to be able to demonstrate compliance.

They first of all have to comply in general with the **main principles** listed in Article 5 of the GDPR (Lawfulness, fairness, transparency / Purpose limitation / Data minimization / Accuracy / Storage Limitation / Integrity & Confidentiality).

Moreover, the GDPR imposes several **specific obligations** on controllers and, to some extent, on processors, which are intended to help them comply with these main principles (for instance, obligations of data protection by design and by default, obligations to keep records of data processing, the obligation to perform data protection impact assessments, the obligation to appoint a Data Protection Officer, etc).

Data subjects receive several new rights (for instance, an extended right to receive information when their data is collected) and these will result in additional obligations for controllers and processors.

Risks and Sanctions

- Supervisory authorities will have significant **corrective powers**, *e.g.,* to carry out audits and instigate processing bans.
- **Fines** of up to the greater of €20 million or 4% of a company's total annual global turnover may be awarded in case of non-compliance.
- Members States will be free to adopt other **civil or criminal sanctions** for infringement of the GDPR.
- Data controllers and processors could be held liable for **damage claims** brought by data subjects (including class actions).

Action Points

- Review current data processing activities, verify obligations under the GDPR and make a gap analysis.
- Identify action points.
- Implement necessary new policies and procedures.

Data Security & Data Breach Reporting Duty

Controllers and processors have to ensure an appropriate level of security through technical and organizational measures, which have to be tailored to the respective processing situation.

The GDPR obliges controllers to report data breaches to the authorities, in principle within 72 hours. Affected data subjects have to be informed as well, if the breach could significantly affect their rights. Processors are expressly obliged to report a breach 'without undue delay' to the controller.

International Data Transfers

Where data is to be transferred outside the EU for processing purposes, adequate safeguards have to be in place. If the European Commission has not issued an Adequacy Decision, personal data may still be transferred under mechanisms such as Binding Corporate Rules or Standard Contractual Clauses. Under the GDPR, transfers will in the future also be legitimized by adherence to Certificates, Seals, or Codes of Conduct to be developed.

This short document provides a general outline of the main provisions of the GDPR. For further details, please contact us for a copy of our GDPR brochure or speak directly to our Brussels experts:

Key Professionals (Brussels)

Maarten Stassen
Partner
T: +32.2.214.28.37
E: mstassen@crowell.com

Frederik Van Remoortel
Partner
T: +32.2.282.18.44
E: fvanremoortel@crowell.com

Emmanuel Plasschaert
Partner
T: +32.2.282.40.84
E: eplasschaert@crowell.com

Key Professionals (Washington, D.C.)

Jeffrey Poston
Partner
T: +1.202.624.2775
E: jposton@crowell.com

Jeane Thomas
Partner
T: +1.202.624.2877
E: jthomas@crowell.com

Industries Affected

For HR data protection issues: all industries.

Specific Industries at Risk

- Automotive
- Financial Institutions
- Healthcare
- Hospitality & Leisure
- Retail & Consumer Technology
- Media & Telecommunications

Notable Rankings

Crowell & Moring's team 'possesses deep knowledge of and experience with data breach response, as well as very practical guidance on how to apply legal solutions to business problems'. The 'pragmatic' group handles GDPR compliance issues for clients operating in industries such as automotive, life sciences, healthcare, TMT and energy.

Legal 500 EMEA, 2021