Data. Protection. Adding Value.

Data Protection Laws - European Union

Legislation

Data protection law within the EU and the EEA was harmonized by the Regulation (EU) 2016/679, more commonly known as the **General Data Protection Regulation** or short "GDPR" which came into force on 25 May 2018. The GDPR provides a detailed set of rules applicable in all EU and EEA countries but is supplemented by local implementation legislation (see "**GDPR Local Insights**").

Scope: The GDPR applies to the processing of personal data, i.e. any information relating to an identified or identifiable natural person, unless the processing is intended for purely personal activities. The scope of the GDPR also **extends** to controllers/processors **outside of the EU** where the processing is related to (i) an offering of goods or services to an individual within the EU, or (ii) the monitoring of individuals in the EU.

Exemptions: The GDPR allows members states to deviate in certain instances from the general rules. For further details, please refer to "**GDPR Local Insights**".

Risk Level: High

Supervisory Authority

Supervisory Authority: Compliance with the GDPR is overseen by the local data protection authorities in the respective member state where the processing is conducted. In case of cross-border processing, the supervisory authority of the main establishment will be designated as lead authority.

Registration/Approval Requirements: No. - There is no requirement for a controller or processor to registered with the competent supervisory authority. Approval requirements, however, may apply to certain instruments available under the GDPR, such as Binding Corporate Rules which may be used as a data transfer mechanism (see "Cross-Border Transfers"). Consultation with a supervisory authority might be required in connection with data protection impact assessments if a high risk has been identified.

Enforcement

Fines: The GDPR allows supervisory authorities to issues **fines up to 20 million euros** or, in the case of a company, **up to 4% of the total annual global turnover** achieved in the previous financial year, whichever is higher. In addition to fines, other corrective powers are available, including to the power to impose a temporary or definitive limitation, e.g. a ban on data processing.

Remedies for Individuals: Individual may complain to the competent supervisory authority which then is obliged to conduct a formal investigation to an appropriate extent, but also seek judicial relief. This includes claiming **compensation for material and non-material damages** that may have been suffered as a result of an infringement.

General Data Privacy Principles

The GDPR sets out certain general principles that must be complied with when processing personal data. This includes:

- **Lawfulness, fairness and transparency**: Personal data must be processed lawfully, fairly and in a transparent manner.
- **Purpose limitation**: Personal data may only be processed for a specified and legitimate purpose, secondary use of data is only allowed under specific circumstances.
- **Data minimisation**: Processing must be restricted to what is strictly necessary to achieve the processing purposes, i.e. only such data must be collected and processed that necessarily required.
- **Accuracy**: It must be ensured that the personal data is accurate and up-to-date, otherwise erased or rectified.
- **Storage limitation**: Personal data must only be stored as long as it necessarily required for the processing purpose, incl. applicable retention obligations.
- **Integrity and confidentiality**: The security and confidentiality of the relevant data must be ensured.

The entity responsible for the processing must be able to demonstrate compliance with such principles ("**Accountability**").

Data Processing

Legal Basis for Processing: The processing of personal data requires a "**legal basis**" for the processing to be lawful. The GDPR identifies the following legal bases: (i) consent, (ii) performance of a contract with the individual, (iii) compliance with a legal obligation, (iv) protection of vital interests, (v) performance of a task carried out in the public interest or in the exercise of official authority and (vi) legitimate interests. In case of legitimate interests, this requires that such interests ultimately outweigh the individual's interest in their right to protect their personal data.

Sensitive Personal Data: Stricter requirements apply to "**special categories of personal data"**, i.e., health data, genetic or biometric data, racial or ethnic origin, political opinions, trade union membership, religion and other beliefs and information about sex life. Processing of such data in the majority of cases may require the consent of the data subject or an explicit statutory requirement (e.g. in the employment context).

Other Restrictions on Processing: Special conditions also apply to the processing of personal data relating to criminal convictions and offences.

Transparency Requirements

Individuals **must be informed** if and to what extent their personal data is being processed. This is also required if the entity processing the information has not obtained the data directly from the person, but through a third party. In practice, the transparency requirements are fulfilled by issuing **data privacy notices**.

pwc

Individual Rights

Individuals have the following rights under the GDPR in relation to the processing of their personal data:

- **Right to access**: obtain information about the personal data stored and the purposes of processing.
- **Right to correction:** request correction of their data.
- **Right to restriction:** request restriction of processing in certain circumstances (e.g., in case the processing is unlawful or the data are not accurate).
- **Right to deletion/be forgotten:** request deletion in certain circumstance (e.g., the individuals has rightfully objected to the processing).
- **Right to portability:** obtain the data in a structured format.
- **Right to object:** object to the processing of their data (i) on basis of legitimate interests on the grounds of their particular situation, (ii) for direct marketing purposes and (iii) for automated decision-making, including profiling.

Other Business Obligations

Data Protection Officer: Entities are required to appoint a data protection officer if (i) they are a public authority or body, (ii) their core activities include regular and systematic monitoring of individuals on a large scale or (iii) their core activities consists of processing special categories of data or data related to criminal convictions and offences on a large scale.

Risk Assessments: A data protection impact assessment is required where a processing activity likely results in a high risk to natural persons, this shall in particular apply where a new technology is introduced. The supervisory authorities have issued "black lists" indicating for which activities they deem a risk assessment to be required.

Audits and Trainings: The data protection officer is responsible to monitor GDPR compliance within an organisation and for awareness-raising and training of staff. Otherwise, audits and trainings are not explicitly statutorily imposed, but indispensable for ensuring compliance with the data protection regime and expected by supervisory authorities as a part of the internal data protection framework.

Record Keeping: Entities processing personal data must keep records of their processing activities.

Security & Data Breaches

Security Requirements: Entities processing personal data (as a controller or processor) are required to implement appropriate technical and organisational security measures to ensure a certain level of security.

Data Breaches: Data breaches must be **reported** to the competent supervisory authority **within 72 hours**, unless the data breach is unlikely to result in a risk to the natural persons that are affected. In the event of a high risk, the controller must also notify the affected natural persons of the data breach.

Service Providers & Cross-Border Transfers

Service Provider Arrangements: Where an entity engages a processor to process personal data on its behalf, this requires the implementation of a **data processing agreement** with specific content prescribed by the GDPR. A **joint controller agreement** is required where two parties jointly determine the means and scope of the processing.

Cross-Border Data Transfers: The EU Commission recognizes a set of countries (e.g. Canada, the UK and Switzerland) as having an adequate level of data protection. Transfers to such countries are not restricted. The transfers of personal data to other countries outside the EU requires a data transfer impact assessment and the implementation of additional safeguards which ensure an appropriate level of data protection, such as Standard Contractual Clauses.

To Watch

International data transfers have been on the watchlist of the supervisory authorities in the recent years. Whereas with the implementation of EU-US Data Privacy Framework allowing data transfers to companies certified under the regime without additional safeguards the main issues appears to be resolved, with the importance of global delivery chains this remains a hot topic. Another focal point is the increasing use of KI-based technologies which not only utilizes large sets of personal data for training purposes, but provides whole new possibilities for data processing use cases.

pwc

RITM8650648