Overview of the EU General Data Protection Regulation (GDPR)

Fines of up to €20,000,000 or up to 4% of annual worldwide turnover, whichever is higher

Personal Data

''Is processing personal data allowed?'

Lawfulness of processing personal data Lawful when unambiguous consent is given; necessary for the performance of a contract; performing a legal obligation; protecting vital interests; carrying out tasks in the public interest or for the purpose of a legitimate interest. Legitimate interest no longer applies to public authorities.	6
Principles applicable to processing of personal data Lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability.	5
Demonstrable consent for certain purposes (if consent is used as the legitimate ground for the processing) Organisations must be able to demonstrate they have consent to process personal data. Consent can be withdrawn at any time. Provisions are considered non-binding in case of non-compliance with the rules. Written consent requests must be clear and separated from other matters.	7
Transfer of personal data Transfer outside the EU is only permitted under certain conditions. Multi-nationals can draft binding corporate rules that need approval from a competent supervisory authority.	45-47
Special categories of personal data (such as ethnicity, political opinions, religious beliefs, health, sexual orientation) The processing of special categories of personal data is prohibited or subject to strict conditions.	9
Additional protection for children under 16 Processing of personal information from children under 16 is only allowed with consent given or authorised by the holder of parental responsibility over the child. Organisations must make reasonable efforts to verify the consent, taking into consideration available technology.	8
Profiling Profiling with legal effects is only permitted under certain circumstances. If profiling significantly affects the data subject, he/she has the right not to be subject to such a decision if it is solely based on automated processing.	22
Exception for certain purposes The Regulation does not apply to archiving for purposes in the public interest and scientific, historical or statistical purposes.	5/89

Maintenance

'How to conduct privacy maintenance?'

Implementation and documentation Organisations must, amongst others, analyse the processing carried out by themselves or their suppliers, the kinds of data subjects, the purposes of the processing and security measures taken. In some cases, organisations must maintain a record of processing activities.	5/24/30
Check, review and conclude Data Processing Agreements Processing of personal data is governed by a contract (data processing agreements) between controller and processor.	28/29
Risk analysis and DPIA (DPIA/compliance review) A risk analysis must be performed for existing and new services. For high risk services or systems a Data Protection Impact Assessment (DPIA) must be conducted.	24/35
Information security Organisations must take appropriate technical and organisational measures to protect personal data.	24/32/35
Managing consent and rights of data subjects Systems and processes will need to be designed and managed to meet the rights of data subjects, such as the right of access, rectification and the "right to be forgotten".	7/15-19
Data portability Data subjects have the right to obtain a copy of their personal data in an electronic and usable format.	20
Policies and the implementation of technical and organisational measures Organisations should develop policies and must be able to demonstrate the use of appropriate technical and organisational measures in order to show compliance and transparent processing of personal data.	24/32
Retention Limit the storage period and delete or archive (if permitted) data in a timely manner.	5/89

Organisation

'How to embed privacy in your organisation?'

Data Protection Officer In some cases, organisations need to appoint a data protection officer, for example when public bodies or authorities carry out the processing, when processing is a core activity or when large amounts of special personal data are processed.	37-39
Rights of data subjects (access, correction, deletion, compensation, objection) Implement processes for exercising rights. Data subjects may request information about processing purposes, categories of data, recipients, and retention, and they can request rectification or erasure. Data subjects have the right to file a complaint and can object to automated decision-making (profiling).	15-18/21/22/24
Data breach notifications Implement procedures for data breach notifications.	33/34
Trained staff and a privacy aware organisation To minimise risks, organisations and their employees should be aware of the key elements of the legislation and act accordingly.	5/24/28
Relevance of privacy for (developing) products and services (data protection by design/default) Include privacy in the development of new products and services.	25
Certification Organisations are encouraged to become certified for privacy (to demonstrate compliance). A certificate may be issued by certification bodies accredited by the supervisory authority and/or the national accreditation body.	42/43/83
Supervision The supervisory authority in the country of the main establishment of the organisation will be responsible for supervision.	56/60

Communication

'How to communicate about privacy?'

Clear and comprehensible communication regarding data Information and communication about the data processing, the rights of data subjects and the privacy statement should be understandable and should be drafted in plain (common) language, especially when it is directed at children.	7/8/14/15/21
Data breach notification to supervisory authority and stakeholders Data breaches must be reported to the supervisory authority within 72 hours and in some cases require immediate notification to the data subjects concerned. If the notification to the supervisory authority is not made within 72 hours, reasons for the delay must be indicated.	33/34
Contact details of Data Protection Officers (DPOs) Contact details of the DPO must be published and sent to the competent supervisory authority. Stakeholders must be able to contact the DPO in order to exercise their rights.	37
Communication with the supervisor The supervisor may request documents and information and has the power to gain access to all personal data and the locations where they are stored.	31/58
Objection to profiling Data subjects must be informed explicitly about their right to object to profiling.	22
Openness about record of processing activities On request, the record must be made available to the supervisory authority. Optionally, the record of processing activities or an overview of processing activities can be made public. This enhances transparency and promotes accountability.	30
Information to obtain valid consent If a processing activity is based on consent, clear and comprehensible information regarding the purpose needs to be provided beforehand.	6