

Enhanced rights and new rights

Right to be forgotten, data portability, restriction of processing etc.

Appointment of a Data Protection Officer

Mandatory (Art. 37) or strongly recommended.

A single regulatory framework

directly applicable from May 25, 2018 in all EU member states.

Extended scope of application

- Applies to all data processing by a controller/processor based within the EU, even if the data is processed outside the EU.
- Also applies to any processing of data of EU residents, even if the data controller or processor is based outside the EU (extra-territoriality).

Mandatory notice of data breaches

Obligation on data controllers to notify data breaches to the supervisory authority without undue delay and where feasible, not later than 72 hours after they become aware of the breach, unless there is no risk for the rights and freedoms of the data subjects.









Appropriate technical and organisational measures must be put in place. Data only processed where necessary.





New approach with accountability

Previous approach was based on prior notice/ex-ante controls. New regulation introduces an ex-post control system. Organisations must therefore be able to demonstrate compliance at all times.



In addition to advisory duties, data processors must now maintain a special record of processing activities and implement "appropriate technical and organisational measures".





Impact assessments

When the data processing is likely to result in high risks to rights and freedoms of the data subjects.

More severe penalties

up to €20,000,000 or 4% of the annual worldwide turnover of the preceding financial year.

Extended definition of sensitive data

Now includes genetic and biometric data. General prohibition on sensitive data processing remains the principle.

A definition of health data

All data related to the health of data subjects, revealing information about their past, present or future physical or mental health.

