

Data protection principles



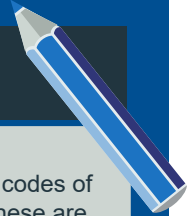
At a glance



- The data protection principles are revised but are broadly similar to the principles set out in Directive 95/46/EC (the “Data Protection Directive”): fairness, lawfulness and transparency; purpose limitation; data minimisation; data quality; security, integrity and confidentiality.
- A new accountability principle makes controllers responsible for demonstrating compliance with the data protection principles.



To do list



Review data protection policies, codes of conduct and training to ensure these are consistent with the revised principles.



Identify means to “*demonstrate compliance*” – e.g. adherence to approved codes of conduct, “paper trails” of decisions relating to data processing and, where appropriate, privacy impact assessments.



Degree of change

Commentary

The principles under the GDPR are broadly similar to those in the Data Protection Directive, but there are some new elements highlighted in italics below.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly, and *in a transparent manner in relation to the data subject*.

Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for *archiving purposes in the public interest*, or scientific and historical research purposes or statistical purposes shall not be considered incompatible with the original processing purposes. However, conditions in Article 89(1) (which sets out safeguards and derogations in relation to processing for such purposes) must be met.

Data minimisation

Personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed.

Accuracy

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation

Personal data must be kept *in a form which permits identification of data subjects* for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for *archiving purposes in the public interest*, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1) and subject to implementation of appropriate technical and organisational measures.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

The controller shall be responsible for and be *able to demonstrate* compliance with these principles.



Where can I find this?

Article 5 and Recital 39