UK GDPR Policy

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (UK GDPR). OTT is responsible for using personal data and has to follow strict rules called 'data protection principles'. These are broad rules about conduct or desired outcomes and are an important part of data protection law, and are, in fact, at the core of the General Data Protection Regulation (UK GDPR).

Whilst UK GDPR is a piece of European Union (EU) legislation, following the transition period it has since been incorporated into UK law and is now known as the UK GDPR. It presents a substantial overhaul of data protection laws, bringing them into line with an increasingly digitised world.

UK GDPR updated for Brexit

The EU General Data Protection Regulation “EU-GDPR”, was established to protect the rights and freedoms of EU Citizens (Data Subjects), with respect to their Personal Identifiable Information (PII) and defined who and how their data could be used and retained by organisation around the world.

On 24th May 2018, one day before the “EU-GDPR” became law across the whole of Europe, the UK Government approved the updated Data Protection Act known as Data Protection Act 2018 (DPA 2018). DPA 2018, was a complete rework of the original ‘Data Protection Act’ of 1998 and incorporated into it, were all the clauses from the “EU-GDPR” and this legislation, therefore, became the basis upon which “Data Protection” would be judged within the United Kingdom.

As the result of Brexit and with effect from the 1st Jan 2021, the UK stopped being part of the EU and hence the “EU-GDPR” cease to protect the rights and freedoms of UK Citizens regarding their Personal Information. To prevent this becoming the case, the UK Government published an update to the DPA 2018 called the ‘Data Protection, Privacy and Electronic Communication’:

The complete guide to UK GDPR can be accessed at uk-gdpr.org

The processing of personal data

Whilst various principles can be found throughout the UK GDPR, Article 5 UK GDPR in particular sets out seven key principles related to the processing of personal data, which controllers (i.e. those who decide how and why data are processed) need to be aware of and comply with when collecting and otherwise processing personal data. These are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability.

Lawfulness, Fairness, and Transparency

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

- **Lawfulness** means that any processing of personal data carried out by a controller must have a legal basis under the UK GDPR, be otherwise compliant with the requirements of the UK GDPR and the 2018 and not involve any otherwise unlawful processing or use of personal data.
- **Fairness** is also a relatively broad principle, which requires that any processing of personal data must be fair towards the individual whose personal data are concerned, and avoid being unduly detrimental, unexpected, misleading, or deceptive.
- **Transparency** is a particularly important principle of data protection within the UK GDPR, with various related rights and obligations seeking to ensure that processing of personal data is clear and transparent to individuals and regulators. Controllers must provide individuals with information regarding the processing of their personal data in a format that is concise, easily accessible, easy to understand, and in clear and plain language. This should be done before personal data are collected and subsequently whenever changes to the processing operation are made. In order to be transparent, controllers must ensure the means of conveying information is the most appropriate for their platform and target audience. In particular, the principles of fair and transparent processing require that the individual be informed of the existence of the processing operation and its purposes.

Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes, which are determined at the time of the collection of the personal data, and not be further processed in a manner that is incompatible with those purposes.

Data Minimization

This principle requires that controllers only collect and process personal data that are adequate, relevant, and limited to what is necessary for the purposes for which they are processed. This essentially means that data controllers should collect the minimum amount of data they require for their intended processing operation; they should never collect unnecessary personal data. This principle complements, in particular, the principle of purpose limitation, but also supports compliance with the range of data protection principles.
The UK GDPR does not define what amount of personal data is ‘adequate, relevant and limited’. This will have to be assessed by controllers depending on the circumstances of their intended processing operations. OTT periodically reviews the amount and nature of personal data which they process, ensuring it remains adequate, relevant, and necessary, including by deleting data which no longer fulfil these criteria.

Accuracy

This principle requires that controllers ensure personal data are accurate and, where necessary, kept up-to-date. Controllers should take every reasonable step to ensure that personal data which are inaccurate are erased or rectified without delay, having regard to the purposes for which they are processed. OTT have clear procedures for correcting or erasing any inaccurate personal data as part of their data management activities.
OTT has obligations in relation to data subjects' right to rectification – to have inaccurate personal data rectified, or completed if it is incomplete.

Storage Limitation

OTT hold personal data, in a form which permits the identification of individuals, for no longer than is necessary for the purposes for which the personal data are processed.
The UK GDPR recommends that time limits should be established by the controller for erasure or for a periodic review. In line with the principle of transparency, controllers should also
ensure that individuals are aware of retention periods or the criteria used to calculate them.

Integrity and Confidentiality

Personal data must be processed by controllers only in a manner that ensures the appropriate level of security and confidentiality for the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. To achieve this end, controllers must utilise appropriate technical or organisational measures. OTT ensure that their security measures adequately protect against accidental or deliberate harm, loss, or dissemination of the personal data they process. These security measures cover not only cybersecurity but also physical and organisational security measures. OTT routinely check that their security measures are up-to-date and effective. The UK GDPR does not specify the security measures which organisations should implement, as technological and organisational best practices are constantly evolving.

Accountability

The principle of accountability is a new principle of data protection law, which specifically sets out that controllers are responsible for, and must be able to demonstrate compliance with the other principles of data protection. This means that controllers need to ensure they comply with the principles, but also have appropriate processes and records in place to demonstrate compliance. Obligations under the principle of accountability are ongoing and evolving.

December 2025
Reviewed by: RI

Review date: December 2026