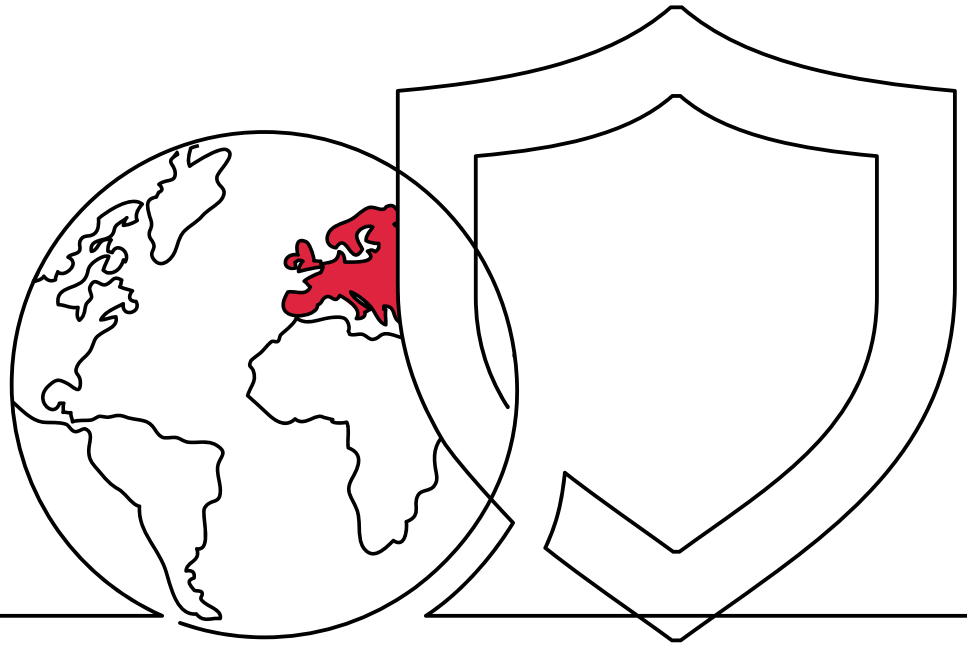
Oury Clark Quick Guides:

Oury Clark

General Data Protection Regulation

(GDPR)



Data Protection: C21

The GDPR came into force on 25 May 2018 with the intention of harmonising European data protection laws with the demands and challenges of 'big data'.

Following Brexit, the GDPR will remain in force in the UK and has been implemented into UK law. Further, the EU has indicated that they will formally grant the UK "equivalence" which will enable the free movement of data between the EU and the UK to continue.

This Quick Guide intends to cover some of the major points of the GDPR, but we strongly recommend someone in your organisation takes responsibility in overseeing your business' compliance with GDPR and UK data protection and you consult advisers or solicitors to assist along the way.

Who does the GDPR apply to?

The GDPR applies to any business, whether established inside or outside of the EU, that offers goods or services to people in the EU (including employment) or monitors behaviours of anybody located within the EU.

Key Definitions

Personal Data is information that relates to a living individual who can be directly or indirectly identified through this data. This could be a name, address, email, ID number, ethnicity, gender, and IP address to name a few.

Controller – determines the means and purposes of processing Personal Data.

Processor – processes Personal Data on behalf of, and on the instruction of, the Controller.

Data Subject – this is the living individual whose Personal Data is being processed, e.g. customers, clients, employees, website visitors.

Processing – almost any activity involving Personal Data, including collecting, recording, storing, amending, disclosing or even destroying Personal Data.

Data Protection Principles

Wherever Personal Data is processed, it must be in accordance with the seven protection and accountability principles. The Controller is responsible for and must be able to demonstrate compliance with all of the data protection principles.

When is Personal Data allowed to be processed?

Personal Data can only be processed if one of the following legal basis is in place:

- The Data Subject has given specific, unambiguous consent to process their Personal Data.
- Processing is necessary to perform a contract with the Data Subject.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary to protect the vital interests of the Data Subject or another person (e.g. to save someone's life).
- Processing is necessary for the performance of a task carried out in the public interest or to exercise official authority (note this is not often relevant to private businesses).
- Processing is in the data controller's legitimate interests except where such interests are overridden by the interest, rights or freedoms of the Data Subject.

For most private businesses, there is likely to be consideration of both performance of a contract and legitimate interests as the legal basis for processing.

Data Subject Privacy Rights

The GDPR recognises various privacy rights for Data Subjects, which aim to give individuals more control over their Personal Data.

Access to data is a key right and one that often causes the most problems for businesses.

Security and Breach Reporting

An organisation is required to raise reportable Personal Data breaches or security incidents to the regulator within 72 hours of becoming aware of it.

Systems, procedures and policies should be in place to ensure consistent monitoring and the ability to rapidly report data breaches or security incidents.

Penalties, Enforcement Action and Claims

The maximum fine under the GDPR is up to 4% of annual global turnover or €20 million, whichever is greater.

The UK's supervisory authority, the ICO (Information Commissioner's Office) also has a range of investigative, corrective and advisory powers to ensure compliance with the GDPR.

Compensation

Individuals can bring claims for compensation and damages against both controller and processors where there is a breach of the GDPR.

A controller may be liable for damage (including for material damage such as distress) caused by its breach of the GDPR. The same is true for processors where it is a processor at fault for damage caused in breach of its own GDPR obligations.

What should businesses be doing?

Controllers must be able to demonstrate that they, and their supply chain, are GDPR-compliant, and this can be used as a very attractive marketing tool to boost confidence amongst customers and partners alike.

Some preliminary steps to take to assist achieving this include:

- Ensure your business is registered with the ICO (if applicable).
- Designate data protection responsibilities to a specific individual or team.
- Identify what Personal Data the business processes. Understanding where it comes from, where it goes, where it resides, what value the data has and who is responsible for it.
- Create a security strategy and implement policies to enable the business to protect data, secure access to it and have the means to erase it.

Let us Introduce Ourselves

Email: contact@ouryclark.com

Oury Clark London:
10 John Street, London WC1N 2EB

Tel: +44 (0) 20 7067 4300

Oury Clark Slough:
Herschel House, 58 Herschel Street
Slough SL1 1PG

Tel: +44 (0) 1753 551111

How we can help

It is a legal requirement to have up-to-date GDPR-compliant Privacy Notices in place that apply to your services. We can assist in reviewing or drafting an appropriate Privacy Notice for your business.

When transferring Personal Data outside of Europe, we can assist with drafting a transfer agreement and Standard Contractual Clauses to meet the standard of GDPR.

Our legal team can advise on any compliance, breaches, data subject access requests, ICO investigations and any other data protection concerns you may have.