# General Data Protection Regulation (GDPR)

## Table of Contents


Table of Contents ..... 1
1.Overview ..... 2
2.General Data Protection Regulation (GDPR) ..... 2
2.1 What is GDPR? ..... 2
2.2 What is ‘personal data’? ..... 2
2.3 GDPR Amendments ..... 3
3.Data Protection and Digital Information Bill (DPDI) ..... 3
3.1 What is the UK Data Reform Bill? ..... 3
3.2 What are the key objectives of the DPDI Bill? ..... 4
3.3 Simplification of data protection processes for users ..... 4
3.4 Use of Personal Data for Research and Enovation ..... 4
3.5 Modernising the Information Commissioner’s Office (ICO) ..... 5
3.6 International Data Sharing ..... 5
3.7 Future-Proofing Legislation for Emerging Technology ..... 6
4.EU AI Act ..... 6
4.1 What is the EU AI Act? ..... 6
4.2 Risk Classification ..... 7
5.ePrivacy Regulation ..... 8
5.1What is the ePrivacy Regulation? ..... 8
5.2 What are the objectives of the ePrivacy Regulation? ..... 8

## 1. Overview

**Jurisdictional Focus:** United Kingdom (UK) and European Union (EU)

Lawful Basis for Processing: Articles 6-9

Data Subject Rights: Articles 12-23

Data Breach Notification: Articles 33-34

Cross-border Transfers: Articles 44-50

## 2. General Data Protection Regulation (GDPR)

### 2.1 What is GDPR?

The EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 are the two governing bodies for personal data in the UK. This regards the acquisition, holding and use of personal data. The Information Commissioner's Officer (ICO) is the regulating body and provides guidance for compliance regarding GDPR.

The ICO's guide on GDPR: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

Organisations responsible for processing personal data must ensure compliance with new regulations through Data Protection Officers.

### 2.2 What is 'personal data'?

Personal data is data

**General Data Protection Regulation (GDPR)**

- Article 3(1) of the GDPR provides that the "Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."
- Article 3(1) GDPR refers not only to an establishment of a controller, but also to an establishment of a processor. As a result, the processing of personal data by a processor may also be subject to EU law by virtue of the processor having an establishment located within the EU.
- Article 3(1) ensures that the GDPR applies to the processing by a controller or processor carried out in the context of the activities of an establishment of that controller or processor in the Union, regardless of the actual place of the processing.

**General Data Protection Regulation (GDPR)**

The European Commission adopted a new set of Standard Contractual Clauses (which came into effect on 27 June 2021) for the transfer of personal data to non-EU regions ("New SCCs"). From 27 September 2021 onwards, data exporters and data importers can only conclude contracts incorporating the New SCCs for the transfer of personal data out of the European Union.

**General Data Protection Regulation (GDPR)**

An organisation or business is likely to be considered to have an EU "establishment" if it exercises "any real and effective activity", even a minimal one, through "stable arrangements" in the EU (See Weltimmo v. NAIH, Case C-230/14)

**General Data Protection Regulation (GDPR)**

Factors such as the use of a language or a currency of one or more Member States in ordering goods and services, may make it apparent that the data controller envisages or targets at offering goods or services to individuals in the EU, and hence be caught by the GDPR.

**General Data Protection Regulation (GDPR)**

The GDPR expressly incorporates an accountability principle under Article 5(2): Organisations / businesses are required to:

- demonstrate their compliance with the principles of processing of personal data;
- implement appropriate technical and organisational measures to ensure compliance; and
- integrate data protection into their processing activities.

**General Data Protection Regulation (GDPR)**

- Under Art 33, it is mandatory for organisations and businesses to give data breach notification. - introducing direct regulation of data processors

They are required under the GDPR to notify the supervisory authority in the EU Member States of a data breach without undue delay (and where feasible, no later than 72 hours after becoming aware of it) unless the breach is unlikely to result in a risk to the rights and freedoms of individuals (Mandatory Breach Notification Requirement)

## 3. Data Protection and Digital Information Bill (DPDI)

The Data Protection and Digital Information Bill (DPDI), also known as the UK's Data Reform Bill, implemented the 23rd of October 2024.

### 3.1 What is the UK Data Reform Bill?

The Bill is a piece of legislation presented in the United Kingdom that seeks to update and modernise the country's data protection regulations. It is a post-Brexit reform aimed at tailoring the General Data Protection Regulation (GDPR), which was preserved in UK law after leaving the European Union, to better meet the UK's individual requirements while preserving strong data protection standards. It provides a new mechanism, for introducing special categories. For instance, s74, which adds new Article 11A to the UK GDPR).

3.2 What are the key objectives of the DPDI Bill?

- **Simplification of data protection processes**: Simplifying data protection processes for businesses to lessen regulatory requirements, with a focus on small and medium-sized businesses.
- **Use of Personal Data for Research and Enovation**: Enabling a wider use for personal data to be used for scientific research, healthcare, and innovation without undermining individual's rights.
- **Modernising the ICO**: Reforming the Information Commissioner's Office (ICO) to increase its governance powers, responsibilities and accountability to ensure effective enforcement.
- **International Data sharing:** Establishing mechanisms to ensure that international data transfers are secure to foster trade.
- **Digital Verification Services:** Improving the UK's digital economy by building the basis for safe and efficient digital verification systems.

3.3 Simplification of data protection processes for users

- Reduction of Cookie Pop-Ups - The Bill includes amendments to streamline how users manage online tracking preferences, giving websites flexibility while ensuring user choice is preserved.
- Certain types of cookies no longer require user consent such as cookies which are essential for functionality as well as analytics cookies which collect data to improve website performance as long as they do not pose a risk to privacy.
- The Bill promotes developments which would allow users to pre-set their cookie preferences which would avoid repeated pop-ups.
- Organisations must have explicit before making marketing calls or direct messages.
- Marketing callers must display their phone numbers to ensure transparency and allow users to report or block unwanted calls.
- Introduction of increased fines for nuisance calls and text messages from £500,000 to either £17.5 million or 4% of global turnover.

3.4 Use of Personal Data for Research and Enovation

- DPDI makes amendments to some of the GDPR definitions for scientific research and other data processes:
    - Scientific Research:
        - Includes public health, technological innovation and environmental research where the studies are conducted in the public interest.
    - Research-specific Processing:
        - Personal data processing in scientific research is clearly distinguished from general data processing.
- Companies can process personal data without the requirement of consent provided certain safeguards are in place. These include:
    - Organisations must only process data that is necessary for research purposes. Any unrelated data cannot be collected or processed.
    - Personal data must be kept confidential or pseudonymised where possible.

- Encryption, secure storage and control to access must be established to ensure that personal data is protected from unauthorised access.
- Organisations must be transparent to users about how their data will be used for research even when consent is not required. This should include the nature of the research, safeguards put in place by the organisation and any benefits.
- Research that involves the use of AI must involve human oversight unless specific safeguards are in place.
- Research which involves personal data must endure ethical review processes which ensures that the benefit of research outweigh the potential risks of using one's personal data.
- Individuals have the right to object to their personal data being used for research which must be upheld and honoured by organisations.
- The ICO can issue guidance and impose any penalties for breaches of these safeguards.

3.5 Modernising the Information Commissioner's Office (ICO)

DPDI Bill proposes the creation of a statutory board for the ICO to increase its governance powers and operational efficiency (Schedule 15 – The Information Commission).

This involves:

- Appointing a Chair and Chief Executive to lead the board and oversee that all board activities comply with legal standards.
- The board is responsible for ensuring that the ICO fulfils its statutory tasks efficiently while maintaining high data protection standards.
- Board members are appointed through consultation with relevant government departments, such as Science, Innovation and Technology departments subject to their professional expertise regarding data protection law and technology policies.
- Board members must remain impartial and can be removed from office in cases of misconduct, incapacity or breach of fiduciary duties.
- The Bill addresses conflict resolution mechanisms which include a public register of member's to guarantee transparency and the requirement for members to declare any potential conflict.

3.6 International Data Sharing

- Ensures that international data transfers comply with growing global standards while promoting innovation and trade.
- The Bill modifies the requirements for determining whether another nation, organisation, or territory has an "adequate" level of data protection, allowing for more efficient data sharing agreements.
  This involves giving the Secretary of State the authority to recognise the sufficiency of non-EU states outside current EU frameworks.
- The Bill identifies binding corporate regulations (BCRs), standard contractual clauses (SCCs), and developing technology for safe data transfers.

3.7 Future-Proofing Legislation for Emerging Technology

- Ensures that the UK's legal framework is able to adapt to developing and new technologies such as artificial intelligence (AI), biometrics, and digital verification systems.

  Digital Verification Services

  - The DPDI Bill sets establishes protections for the secure exchange of personal information for identity verification purposes thus ensuring more efficient online transactions can take place.
  - It includes measures that ensure data privacy when sharing by authorities.
  - Safeguards against misuse of digital IDs and requirements for transparency in how data is handled.

  Biometric Data Use

  - The Data Protection Act 2018 sets out further clarity of the use of biometric data which includes facial recognition, fingerprint identification, and voice identification.
  - The Bill defines "biometric data" to mean "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopy data"

  Artificial Intelligence

  - The Bill expands the legal foundation for utilising personal data in AI applications, notably in areas like as healthcare, scientific research, and public safety.
    Organisations utilising AI for choices with "significant effects" must maintain openness and allow for human participation.

## 4. EU AI Act

4.1 What is the EU AI Act?

The AI Act is the first legal framework on AI which provides AI developers with defined standards and commitments for specific AI applications. At the same time, the rule aims to decrease the administrative and financial constraints on businesses, particularly small and medium-sized organisations (SMEs). It is due to come into force in 1st August 2025 and will be applicable two years later with some exceptions; prohibitions will take effect after six months. The European AI Office will be responsible for the overseeing of the Act's regulations amongst the EU member states.

4.2 Risk Classification

- **Unacceptable Risk:** These include AI systems deemed damaging to humans' rights or safety, such as social scoring or systems that exploit vulnerabilities. They are completely outlawed.
- **High Risk:** Systems that are harmful to safety or basic rights (for example, in healthcare, law enforcement, or education) must meet severe standards like as risk assessments, human monitoring, and compliance certifications. This refers to systems where AI is used in:
    - Vital infrastructure such as transport which could put citizen's lives at risk.
    - Educational training which can determine one's access to education or someone's life.
    - Safety components of products such as robot-assisted surgery.
    - Employment systems such as CV-sorting software.
    - Law enforcement which can interfere with one's fundamental rights.
    - Migration or border control management for instance though automated examination of passports.
    - Essential public and private services.
    - Legal administrations such as AI being used to determine court rulings.

- High Risk AI systems must meet strict requirements before they can be implemented. This includes:
    - Appropriate risk assessment and mitigation systems.
    - High-quality datasets feeding the system to reduce risks and biassed consequences.
    - Logging activities ensures traceability of findings, and full documentation is provided to authorities for compliance assessment.
    - Providing clear and enough information to the deployer. Implement human monitoring mechanisms to reduce risk.
    - High levels of robustness, security, and precision.

- **Limited Risk:** This includes applications such as chatbots. These systems must fulfil transparency standards, such as informing users when they engage with AI. This also includes AI generated texts and audio and video content which constitute as deep fakes.

- **Minimal Risk:** These carry no substantial threats and have few commitments, such as those found in video games or spam filters.

## 5. ePrivacy Regulation

### 5.1 What is the ePrivacy Regulation?

The ePrivacy Regulation is an expected EU bill that aims to amend and harmonise the ePrivacy Directive (2002) with the GDPR. Its primary goal is to provide privacy and secrecy in electronic communications, but it has expanded to include current digital services.

5.2 What are the objectives of the ePrivacy Regulation?

- Strengthens Privacy Protection

- Alignment with GDPR

- Enhancement of Consumer Rights

- Adapt to Technological Advances

5.3 Strengthening of Privacy Protection and Enhancement of Consumer Rights

- Websites must obtain explicit consent for any non-essential cookies including analytics or advertising whilst strictly necessary cookies are exempted from this requirement.
- Users will be able to set cookie settings at the browser or software level, potentially minimising the requirement for multiple pop-up consents.
- Websites that restrict customers access to services unless they agree to tracking are illegal, unless the tracking is required to provide the service.
- Metadata, such as location information or call durations, can only be handled with the user's permission or under tight restrictions, such as for payment or to detect network irregularities.
- Access to the content of communications needs specific user agreement.
- Businesses must seek prior authorisation before delivering marketing messages via email, SMS, or other channels. Exceptions include mailings to existing customers that are relevant to comparable services and allow consumers to opt out.
- More transparency regarding unsolicited marketing calls such as requiring the identification of caller numbers.

5.3 Alignment with GDPR

GDPR and the ePrivacy Regulation share similar values:

- Both regulations treat individuals' privacy and personal data as basic rights.

- The ePrivacy Regulation emphasises the significance of gaining express agreement for activities like as cookies and tracking, which is consistent with the GDPR's strong consent requirements for personal data processing.
- Both demand clear and easily accessible information regarding data collection and processing, allowing users to make educated decisions.

- Both regulations follow the same structure for fining organisations who do not comply with the regulations which is up to 20 million euros (16.5 million pounds) or 4% of the organisation’s global annual turnover.

- The ePrivacy Regulation follows GDPR’s rule that if a business outside of the EU offers services to EU residents, then they are obliged to follow the ePrivacy Regulations.

However, the distinctions between the two are:

- GDPR allows for processing based on legitimate interests, but ePrivacy Regulation requires consent for most monitoring and communication-related processing.
  Data protection authorities handle GDPR violations, whilst national telecoms regulators may be involved with ePrivacy Regulation enforcement.
- ePrivacy Regulation includes more protections regarding metadata which includes call duration and geolocation.