



## **General Data Protection Regulation (GDPR)**

### **Introduction**

The GDPR, officially known as Regulation (EU) 2016/679, was adopted on April 14, 2016, and became enforceable on May 25, 2018. It aims to protect individuals' privacy and personal data while simplifying the regulatory environment for international business by providing a unified framework across the EU.

### **The UK's data protection legislation**

Data protection legislation controls how your personal information is used by organisations, including businesses and government departments.

In the UK, data protection is governed by the [UK General Data Protection Regulation \(UK GDPR\)](#) and the [Data Protection Act 2018](#). Everyone responsible for using personal data has to follow strict rules called 'data protection principles' unless an exemption applies.

There is a [guide to the data protection exemptions on the Information Commissioner's Office \(ICO\) website](#).

Anyone responsible for using personal data must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- Race
- Ethnic background
- Political opinions
- Religious beliefs
- Trade union membership
- Genetics
- Biometrics (where used for identification)
- Health
- Sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

### **Your rights**

Under the legislation, you have rights in relation to your personal data, with some exceptions.

These include the right to:

- Be informed about how your data is being used
- Access personal data
- Have incorrect data updated
- Have data erased
- Stop or restrict the processing of your data
- Data portability (allowing you to get and reuse your data for different services)
- Object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- Automated decision-making processes (without human involvement)
- Profiling, for example to predict your behaviour or interests
- If you're concerned about how an organisation is handling your personal data
- Personal data an employer can keep about an employee
- Employers must keep their employees' personal data safe, secure and up to date.



## **General Data Protection Regulation (GDPR)**

Employers can keep the following data about their employees without their permission:

- Name
- Address
- Date of birth
- Sex
- Education and qualifications
- Work experience
- National insurance number
- Tax code
- Emergency contact details
- Employment history with the organisation
- Employment terms and conditions (for example, pay, hours of work, holidays, benefits, absence)
- Any accidents connected with work
- Any training taken
- Any disciplinary action
- Employers need their employees' permission to keep certain types of 'sensitive' data, including:
  - Race and ethnicity
  - Religion
  - Political membership or opinions
  - Trade union membership
  - Genetics
  - Biometrics, for example if your fingerprints are used for identification
  - Health and medical conditions
  - Sexual history or orientation
- Employers must keep sensitive data more securely than other types of data.

### **What an employer should tell an employee**

An employee has a right to be told:

- What records are kept and how they're used
- The confidentiality of the records
- How these records can help with their training and development at work
- If an employee asks to find out what data is kept on them, the employer will have 30 days to provide a copy of the information.
- An employer should not keep data any longer than is necessary and they must follow the [rules on data protection](#).

### **Company Policy-Data Protection**

The company will, during your period of employment, be required to keep and maintain information about employees both manually and on computer.

The company will abide by the requirements of the [UK General Data Protection Regulation \(UK GDPR\)](#) and the [Data Protection Act 2018](#), by maintaining these records only during employment and for a reasonable length of time afterwards.

The company will take all reasonable steps to maintain the security of the information, will not pass it on to third parties without consent of the employee, and will process the information fairly.

**All employees must ensure that information is not left unattended so that those not entitled to view that information may see, hear or copy it or be able to use that information when not authorised to do so.**

The company may be required to keep information about employees' convictions in respect of road traffic prosecutions and information on activities during the working shift collected via vehicle data collection devices.



## **General Data Protection Regulation (GDPR)**

If any employee does not consent to the company keeping any of the above information, the employee should advise the company in writing. The company will then erase any relevant data relating to the employee other than that the company are able to keep under the Data Protection Act 1998.

The company operates CCTV at its premises and the footage where applicable may be used for disciplinary or crime prevention purposes.

### **Confidential information**

The employee shall not use or disclose to any person either during or at any time after their engagement by the Company any confidential information about the business or affairs of the Company, any Clients or any of its business contacts, or about any other confidential matters which may come to the employee's knowledge while providing the Services.

Confidential information means any information or matter which is not in the public domain, and which relates to the affairs of the Company, Clients or any of their business contacts.

Any use or disclosure authorised by the Company or as required by law and any information which is already in, or comes into, the public domain otherwise than through the Contractor's unauthorised disclosure.

### **Intellectual Property**

All documents, manuals, hardware and software provided for the employee's use by the Company, and any data or documents (including copies) produced, maintained or stored on the Company's computer systems or other electronic equipment (including mobile phones if provided by the Company), remain the property of the Company

The Company hereby grants the employee a limited personal non-exclusive, non-assignable, non-sublicensable, royalty free licence to use any Company Software solely to the extent necessary to carry out the Services.