1. Important definitions used in the GDPR

Data subject is the identified or identifiable living individual to whom personal data relates.

Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data means any information relating to an identified or identifiable living individual. An identifiable living individual means a living individual who can be identified, directly or indirectly, in particular by reference to either of the following:

a) An identifier such as a name, an identification number, location data or an online identifier.

b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Special Categories of Personal data (known as sensitive personal data under DPA 1998)

a) Racial/Ethnic origin

b) Political opinions

c) Religious or philosophical beliefs

d) Trade union membership

e) Genetic data

f) Biometric data

g) Health

h) Sex Life/sexual orientation

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

2. Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

The data protection principles are:

- **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 only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimisation**. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This represents a stricter requirement than that under the DPA 1998, which provides that the data must not be "excessive" in relation to the purposes for which it is processed. This is likely to make it more difficult for data controllers to collect data for a general or a possible future use.
- **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 is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay. By comparison with the DPA 1998, the new regime includes an express requirement for timely removal or correction of inaccurate data.
- **Storage limitation**. Personal data which is kept in a form which permits identification of data subjects must be kept for no longer than is necessary for the purposes for which the data is processed. There are exceptions to this principle which permit personal data to be stored for longer periods where it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (and then only if there are appropriate technical and organisational measures to safeguard the rights and freedoms of data subjects).
- **Integrity and confidentiality**. Personal data must be processed in a manner that, through use of technical or organisational measures, ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- **Accountability**. The data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles. This is a new principle which does not have an equivalent under the DPA 1998

General Data Protection Regulation

3. Lawful Basis for Processing Personal Data

1. Consent

a. Many employment contracts include a standard clause stating that the employee consents to the employer processing their personal data.

b. Under the GDPR, consent must be freely given, specific, informed and unambiguous. Employees will also be able to withdraw their consent at any time. These requirements are more onerous than under current legislation.

c. In an employment relationship where the balance of power may be unequal, there is a question as to whether an employee can give genuine consent to processing.

d. Article 29 Working Party: "consent will be invalid where there is a clear imbalance between the data subject and the controller."

e. Practical points

i. Given the difficulties of consent in the employment context, processing by employers may be better carried out under a different basis (see below).

ii. Employers who will rely on consent as a lawful basis for processing employee personal data after May 2018 will need to review their consents to assess whether they are GDPR compliant.

iii. You should consider separating consents from standard employment documents such as the employment contract and handbook.

iv. Ensure that the employee is informed of the processing activities that the consent would cover and be clear that the employee is free to refuse their consent without repercussions.

2. Contract

a. You have a lawful basis for processing if you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract.

b. For example, an employer will need to process an employee's personal data for the purposes of paying wages.

3. Legal Obligation

a. You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.

b. For example, an employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC.

4. Legitimate Interest

a. Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact.

b. To rely on this basis an employer needs to:
- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

c. The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

d. The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

e. You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

f. This basis is relevant to matters such as employee monitoring.

g. Details of your legitimate interest must be included in your Privacy Notice.

h. NB – public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

5. Vital Interest

a. You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.

b. The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.

c. You cannot rely on vital interests for health data if the individual is capable of giving consent, even if they refuse their consent.

d. Limited use in an employment context.

6. Public Task

a. Only relevant for public bodies.

b. The Data Protection Act (when passed) will define 'public authority' but it is likely that if you are a public authority as defined under the Freedom of Information Act 2000, you will be a public authority for the purposes of the GDPR.

c. Public bodies can rely on this basis where the processing is necessary to perform a task in the public interest or for official functions and the task or function has a clear basis in law.

d. ICO example :

A university that wants to process personal data may consider a variety of lawful bases depending on what it wants to do with the data.

Universities are likely to be classified as public authorities, so the public task basis is likely to apply to much of their processing, depending on the detail of their constitutions and legal powers. If the processing is separate from their tasks as a public authority, then the university may instead wish to consider whether consent or legitimate interests are appropriate in the particular circumstances. For example, a University might rely on public task for processing personal data for teaching and research purposes; but a mixture of legitimate interests and consent for alumni relations and fundraising purposes.

The university however needs to consider its basis carefully – it is the controller's responsibility to be able to demonstrate which lawful basis applies to the particular processing purpose.

4. Special Category Data

The general prohibition on the processing of the special categories of personal data does not apply where one of the following conditions is met (and the data controller has a lawful basis for processing):

- Where the data subject has given explicit consent.

- Where it is necessary for carrying out rights and obligations under employment law. Examples include:

  - To ensure the health, safety and welfare at work of workers. For example, reviewing night worker health assessment records to monitor compliance with the Working Time Regulations 1998.
  - To ensure a safe working environment.
  - To check the entitlement of workers to work in the UK.
  - To select safe and competent workers.
  - Not to discriminate on the grounds of sex, race, disability, religion or belief, sexual orientation or age (for example, processing equal opportunities monitoring forms).
  - To ensure the reliability of workers who have access to personal data.
  - To maintain records of statutory sick pay, statutory maternity, paternity, shared parental and adoption pay.
  - To protect customers' property or funds in the employer's possession. This would include data collected in the process of security monitoring.
  - To provide employee liability information under TUPE to the potential purchaser of a business.

  However, where this condition is relied, on the employer is obliged to have an appropriate policy in place which explains the employer's procedures for complying with the data protection principles in connection with the processing of the data and explains the employer's policies as regards to the retention and erasure of personal data processed, giving an indication of how long such personal data is likely to be retained.

- Where it is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving consent.

- Where it is carried out with appropriate safeguards in the course of the legitimate activities of a foundation, association or other not-for-profit body which has a political, philosophical, religious or trade union aim. The processing must only relate to members or former members of that body, or persons who have regular contact with it, in connection with its purposes. Personal data must not be disclosed to anyone outside that body without the data subject's consent.

- Where it relates to personal data which has been manifestly made public by the data subject.

- Where processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity.

- Where processing is necessary for reasons of substantial public interest.

- Where processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

- Where processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

- Where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

5. Data Processing Contracts

The GDPR requires data processors' activities to be governed by a "contract or other legal act under Union or Member State law" that sets out:

- The subject matter and duration of the processing.
- The nature and purpose of the processing.
- The type of personal data processed and the categories of data subjects.
- The obligations and rights of the data controller.

In addition, the GDPR requires that data processing contracts obligate the processor to:

- Process personal data only on documented instructions from the controller including with regards to cross-border data transfers, subject to certain limited exceptions.
- Impose confidentiality obligations on all personnel authorized to process the personal data.
- Ensure the security of the personal data that it processes.
- Abide by the rules regarding appointment of sub-processors.
- Implement measures to assist the data controller in complying with data subjects' requests.
- Assist the controller in ensuring compliance with the data security requirements taking into account the nature of the processing and the information available to the processor.
- At the controller's election, either return or destroy the personal data at the end of the relationship, unless EU or Member State law requires a longer retention period.
- Provide the controller with all information necessary for the data controller to demonstrate compliance with the GDPR's obligations relating to engaging data processors. The data processor must notify the data controller immediately if it believes that any instructions from the data controller to provide information violate the GDPR or any other EU or local law.

6. What Information should be included in your Privacy Notice?

The GDPR sets out the information that you should supply and when individuals should be informed.

The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The table below summarises the information you should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓

Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third parties and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	

The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓
When should information be provided?	At the time the data is obtained.	Within a reasonable period of having obtained the data (within one month) If the data is used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

7. Restricting Processing

You will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.

- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.

- When processing is unlawful and the individual opposes erasure and requests restriction instead.

- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

8. Practical considerations to check compliance

- Undertaking an audit to ascertain what personal data you hold, where it came from, how you store it, who you may share it with and what you do with it. You will need to understand how your organisation deals with personal data before you can consider how to ensure that your processes are GDPR compliant.

- Identify lawful bases for processing and document them.

- Where consent is relied upon for processing, consider whether other lawful bases may be more appropriate. If consent is to be relied upon, consider how to deal with an employee withdrawing their consent.

- Put together Privacy Notices and consider how you will issue this to relevant parties.

- What information will you need to include in your Data Protection policy? How will you issue the policy to staff?

- What other processes and procedures will need to be implemented for example:
    - Dealing with subject access requests and other requests that individuals can make under the GDPR;
    - Dealing with data breaches.

- Do you need to update your employment contracts? This is likely to be necessary where consent to processing is included in the contract and where you need to include confidentiality provisions.

- How you will deal with an individual's request to "be forgotten?"

- Are you able to deal with requests relating to data portability?

- Do you need to train staff on GDPR compliance?

- Do you need to update any contract with data processors?