**Personal Data**

‘Personal data’ is information about a “natural” (living) person, making that person identifiable, either directly or indirectly. Examples could include a name, identification number, location, online identifier (IP Address), or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Identifying factors might not necessarily be a single item: there are often occasions where a person becomes identifiable because of multiple factors in one place. For example, if you have a report of an incident that happened in a particular location on a certain date and time, even if the names are changed, people with prior knowledge of the incident are likely to be able to identify who said or did what, based on the details. For this reason, you will never find a definitive list of what IS personal data, as what additional information is available or known will vary between organisations.

**Special Categories of Personal Data**

Sometimes referred to as “sensitive personal data”, Special Category Data is information that might not necessarily identify a person but is a lot more sensitive to that person. These are:

* racial or ethnic origin
* political opinions
* religious / philosophical beliefs
* trade union membership
* genetic data
* biometric data (for identification purposes)
* health data (mental and physical)
* sex life or sexual orientation

**Data Subject(s)**

The Data Subject is the person about whom the personal data relates or identifies.

**Data Processing**

Data Processing is an over-arching term that means “doing something” with personal data. This commonly includes:

* Collecting or collating the data
* Analysing the data
* Sharing the data
* Storing the data
* Destroying the data

**Data Controller**

The Data Controller is occasionally the person or more commonly the organisation with overall responsibility for the processing of personal data that organisation undertakes. They will make all the decisions about what is captured, how it’s used and the purpose for it, as well as deciding what controls need to be in place.

**Data Processor**

A Data Processor is occasionally a person, but more commonly an organisation commissioned by a Data Controller to carry out their data processing on behalf of the Data Controller. These are often software providers such as CPOMS or contracted out services such as an insurance company. Essentially, a Data Processor is acting as an extension of the Data Controller, so must operate under the Data Controller’s instructions, and under the terms of a Data Processing Agreement (contract).

**Data Sharing**

Sharing of personal data means *giving* it to another Data Controller, for them to use for their own purposes. Once you have shared personal data, the recipient becomes the Data Controller for that information and therefore makes the decisions over what they will do with it.

Note, you do NOT share data with your Data Processors, as these are processing it under your Data Controllership.

**Data Breach**

The most common type of data breach is the accidental or unlawful *loss, alteration, destruction, disclosure of or access to* personal data. However, you should consider any failing of one of the Data Protection Principles (Article 5 of UK GDPR) as breach of the UK GDPR Principles, which could include examples such as not having the necessary paperwork in place, not providing the data subject with clear privacy information, retaining personal data for longer than is necessary or processing personal data without an identified lawful basis (Article 6 of UK GDPR).

**Data Profiling**

Profiling’ means any form of *automated processing* of personal data used to evaluate personal aspects relating to a person, in particular to analyse or predict aspects about their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

**Automated Decision Making**

Automated decision-making is the process of *making a decision by automated means* without any human involvement. Automated individual decision-making does not have to involve profiling, although it often will do. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. This is likely to include Artificial Intelligence systems.

The UK GDPR restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

**Data Processing Agreement**

Data Processing Agreements are a legally binding contract between the Data Controller and its Data Processor. This contract defines exactly how the Data Controller expects the Data Processor to process its personal data, and these follow standard contract clauses.

**Data Sharing Agreement**

A Data Sharing Agreement is a non-legally binding written agreement between Data Controllers where there is regular sharing of personal data. The Sharing Agreement should define who is involved in the agreement, what data is being shared, why the recipient needs the data, how this is lawful, and how the data will be shared.

**Joint Data Controllers**

There are occasions when a Sharing Agreement can be quite complicated, because all the organisations have a shared interest in the information, and share a common purpose for the processing. An example could be a regional health initiative, where care records are shared between Local Authorities, as the patients may access health services in neighbouring counties. In this instance, all the Care providers will have a shared interest in the information, making them Joint Data Controllers.