# UK-General Data Protection Regulation Policy– Front Sheet

| | |
|---|---|
| Author / Responsible Director | Head of IT/CEO |
| Review date | May 2023 |

Status control

| | | |
|---|---|---|
| 00 - draft | Head of IT | 2021 |
| 01 - approval by | | |
| 02 - in use from | | |
| 03 - withdrawn | | |

Review control

| Version: | Comments/reviewer: | Date: |
|---|---|---|
| 1 | Reviewed – no amends RM | 26/05/2020 |
| 2 | Reviewed – updates:<br>Head of IT renamed to Head of IT & Systems<br>Supervisory Authority renamed to Commissioner<br>GDPR renamed to UK-GDPR (United Kingdom General Data Protection regulation<br>Update responsibility for ensuring staff have access to training – updated from Head of IT to Managers<br>Remove references to EU articles and directives – updated to UK<br>EU law references renamed to domestic law<br>EU renamed to United Kingdom<br>Responsible Director changed from COO to CEO | 01.06.2021 |
| 3 | | |

**Contents:**

## 1. Introduction

1.1 Background to the United Kingdom General Data Protection Regulation ('UK-GDPR')

Effective from January 31, 2020 the UK has its own version of GDPR known as UK-GDPR.
The United Kingdom General Data Protection Regulation (UK-GDPR) purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used by the organisation (drawn from the UK-GDPR)
Material scope (Article 2) – the UK-GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the UK-GDPR will apply to all controllers that are established in the United Kingdom who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers in the United Kingdom that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the United Kingdom.

1.3 Article 4 definitions

Establishment – the main establishment of the controller in the United Kingdom will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the United Kingdom will be its administrative centre.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – 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; where the purposes and means of such processing are determined by domestic law, the controller or the specific criteria for its nomination is provided for by domestic law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the Commissioner for the United Kingdom and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

## 2. Policy statement

2.1 Spurgeons Board of Directors and management are committed to compliance with all relevant UK law in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Spurgeons collects and processes in accordance with the United Kingdom General Data Protection Regulation (UK-GDPR).

2.2 Compliance with the UK-GDPR is described by this policy and other relevant policies such as the Spurgeons Data Security Policy, along with connected processes and procedures.

2.3 The UK-GDPR and this policy apply to all of Spurgeons personal data processing functions, including those performed by or in relation to working with service users', donors', employees', suppliers' and relevant partners' personal data, and any other personal data the organisation processes from any source.

2.4 Our Board of Trustees are responsible for reviewing this policy and its implementation on an annual basis. This review will be informed by the Head of IT & Systems who is responsible for maintaining a register of processing annually in the light of any changes to Spurgeons activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. The Spurgeons Data Register is available on the Commissioner's request.

2.5 This policy applies to all Employees/Staff and interested parties relevant to Spurgeons such as outsourced suppliers. Any breach of the UK-GDPR will be dealt with under Spurgeons disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate UK authorities.

2.6 Partners and any third parties working with or for Spurgeons, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Spurgeons without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which Spurgeons is committed, and which gives Spurgeons the right to audit compliance data with the agreement.

## 3. Responsibilities and roles under the United Kingdom General Data Protection Regulation

3.1 Spurgeons is a data controller under the UK-GDPR.

<u>The role of senior managers</u>

3.2 Senior Management and all those in managerial or supervisory roles throughout Spurgeons are responsible for developing and encouraging good information handling practices within Spurgeons; responsibilities will be set out in individual job descriptions.

<u>The role of the Data protection Officer</u>

3.3 Spurgeons has a designated individual who is responsible for Data Protection. The role is fulfilled by the Head of IT & Systems and is directly accountable to the Board of Directors of Spurgeons for the management of personal data within Spurgeons and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 Adherence to the UK-GDPR as required by this policy; this will include compliance with this policy on a day-to-day basis including oversight for the compliance of those staff with line management/function responsibility in respect of data processing that takes place within their area of responsibility

3.3.2 security and risk management in relation to compliance with this policy;

3.3.3 specific responsibilities in respect of procedures such as the Subject Access Request Procedure;

3.3.4 being the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

3.4 Spurgeons will ensure that the identity of the designated Data Protection Officer is visible to all employees and has the suitable training, qualifications and expertise to carry out the responsibilities listed above (in 3.3).

3.5 <u>All staff employees and volunteers</u>

3.6 Compliance with data protection legislation is the responsibility of every member of staff (including volunteers) of Spurgeons who process personal data.

3.7 Spurgeons training agreement sets out specific training and awareness requirements that applies to every member of staff. Spurgeons provides essential training on data protection and security and it is compulsory for all staff to undertake this training on an annual basis. If any member of staff is not clear about their responsibilities after this training, they should approach their manager in the first instance. Failure to undertake essential training may be considered a disciplinary issue. Training will be provided both via SLS and/or face to face.

3.8 All staff are responsible for ensuring that any personal data about them and supplied by them to Spurgeons is accurate and up to date.

## 4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the UK-GDPR – detailed below. Spurgeons policies and procedures are designed to ensure compliance with these principles.

4.1 <u>Personal data must be processed lawfully, fairly and transparently</u>

***Lawful*** – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

***Fairly*** – in order for processing to be fair, the data controller has to make certain information available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The UK-GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' principle.

***Transparently*** – the UK-GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;
4.1.2 the contact details of the designated Data Protection Officer;
4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.1.4 the period for which the personal data will be stored;
4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
4.1.6 the categories of personal data concerned;
4.1.7 the recipients or categories of recipients of the personal data, where applicable;
4.1.8 where applicable, that the controller intends to transfer personal data to a recipient to another country and the level of protection afforded to the data;
4.1.9 any further information necessary to guarantee fair processing.

4.2 <u>Personal data can only be collected for specific, explicit and legitimate purposes</u>
Data obtained for specified purposes must not be used for a purpose that differs from those identified in the Spurgeons Data Register.

4.3 <u>Personal data must be adequate, relevant and limited to what is necessary for processing</u>
4.3.1 Ensuring that Spurgeons does not collect information that is not strictly necessary for the purpose for which it is obtained.
4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Head of IT & Systems.

4.3.3 The Head of IT & Systems will ensure that data collection methods are reviewed to ensure that collected data continues to be adequate, relevant, and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 Managers with line management responsibilities are responsible for ensuring staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the data subject to ensure that data held by Spurgeons is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.4 Employees/Staff/Service Users and other relevant partners and suppliers should be required to notify Spurgeons of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Spurgeons to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5 The Head of IT & Systems is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors. The Head of IT & Systems will achieve this by chairing half yearly IT governance meetings that bring together data owners responsible for processing data.

4.4.6 Data will be securely deleted/destroyed in line with the Data Security Policy

4.4.7 Individual data owners are responsible for responding to data rectification requests from data subjects within one month. This can be extended to a further two months for complex requests. If Spurgeons decides not to comply with the request, the data owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the Commissioner and seek judicial remedy.

4.4.8 Make appropriate arrangements that, where third- party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.5.1 Where personal data is retained beyond the processing date, it will be minimised, encrypted and pseudonymised in order to protect the identity of the data subject in the event of a data breach.

4.5.2 Personal data will be retained in line with the timescales detailed in the Spurgeons Data Retention policy and, once its retention date is passed, it must be securely destroyed.

4.5.3 The Head of IT & Systems must specifically approve any data retention that exceeds the retention periods defined in the Spurgeons Data Retention policy. This approval must be documented.

4.6 Personal data must be processed in a manner that ensures appropriate security

The Head of IT & Systems will carry out and review risk assessments considering all the circumstances of Spurgeons controlling or processing operations.

In determining appropriateness, the Head of IT & Systems will also consider the extent of possible damage or loss that might be caused to individuals (staff and service users) if a security breach occurs, the effect of any security breach on Spurgeons itself, and any likely reputational damage including the possible loss of trust.

When assessing appropriate technical measures, the Head of IT & Systems will consider the following (as documented in the Spurgeons Data Security Policy):

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as Windows Information Protection & Azure Rights Management;
- Identifying appropriate security standards relevant to Spurgeons.

When assessing appropriate organisational measures, the Head of IT & Systems may consider the following:

- Any appropriate training levels throughout Spurgeons;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;

- Adopting clear rules about password complexity;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the United Kingdom.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 The controller must be able to demonstrate compliance with the UK-GDPR's other principles (accountability)

The UK-GDPR includes provisions that promote accountability and governance. These complement the UK-GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

Spurgeons will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing appropriate technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

## 5. Data subjects' rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

5.1.3 To prevent processing for purposes of direct marketing.

5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

5.1.5 To not have significant decisions that will affect them taken solely by automated process.

5.1.6 To sue for compensation if they suffer damage by any contravention of the UK-GDPR.

5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

5.1.8 To request the Commissioner to assess whether any provision of the UK-GDPR has been contravened.

5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

5.1.10 To object to any automated profiling that is occurring without consent.

5.2 Spurgeons ensures that data subjects may exercise these rights:

5.2.1 Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how Spurgeons will ensure that its response to the data access request complies with the requirements of UK-GDPR.

5.2.2 Data subjects have the right to complain to Spurgeons related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

## 6. Consent

6.1 Spurgeons understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time only where consent is the legal basis under which data is being stored.

6.2 Spurgeons understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

6.3 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists. The basis for processing will be detailed in the Spurgeons Data Register.

6.4 In most instances, consent to process personal and sensitive data is obtained routinely by Spurgeons using standard consent documents for when an individual signs a contract, or during induction for participants on programmes.

6.5 Where Spurgeons provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13 years.

## 7. Security of data

7.1 All Employees/Staff are responsible for ensuring that any personal data that Spurgeons holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Spurgeons to receive that information and has entered into a confidentiality agreement.

7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Data Security Policy. All personal data should be

treated with the highest security.

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Spurgeons.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with archiving policy and Data & Storage procedures.

7.5 Personal data should be deleted or disposed of in line with the Spurgeons Data Register. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and destroyed before disposal.

7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

## 8. Disclosure of data

8.1 Spurgeons must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff must not disclose personal data held on another individual to a third party without seeking advice.

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Head of IT & Systems.

## 9. Retention and disposal of data

9.1 Spurgeons shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 Spurgeons may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data will be set out in the Spurgeons Data register and retention policy along with the criteria used to determine this period including any statutory obligations Spurgeons has to retain the data.

9.4 Spurgeons data retention and data disposal procedures will apply in all cases.

9.5 Personal data must be disposed of securely in accordance with the sixth principle of UK-GDPR
– processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the Retention Policy

**10. Data transfers**

10.1 All exports of data from within The United Kingdom other countries are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

**11. Information asset register/data inventory**

11.1 Spurgeons has established a Spurgeons Data Register and data flow process as part of its approach to address risks and opportunities throughout its UK-GDPR compliance. Spurgeons data inventory and data flow determines:

- business processes that use personal data;
- source of personal data;
- description of each item of personal data;
- processing activity;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Spurgeons throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

11.2 Spurgeons is aware of any risks associated with the processing of particular types of personal data.

11.2.1 Spurgeons assesses the level of risk to individuals associated with the processing of their personal data.

11.2.2 Data protection impact assessments (DPIAs) are carried out where there is a legal requirement to do so under domestic law.

11.2.3 Spurgeons shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.4 The Head of IT & Systems shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the board and where legally required the Commissioner.

11.2.5 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Spurgeons documented risk acceptance criteria and the requirements of the UK-GDPR.

## Appendix 1

## Glossary of terms

**Commissioner -** This this is the Office of the Information Commissioner.

**Consent** – consent is defined as receiving a data subject's agreement to process their data. Agreement must be freely given, informed, specific and unambiguous. This consent could be given several ways, such as via a written statement (including by electronic means) or an oral statement. Gaining consent must be clear and unambiguous. The data subject must understand implicitly what they are providing their data for, how it will be processed, who will process it and how long it will be stored.

**Data Breach** – any accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access of a subject's data.

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

**Right to be forgotten** – (also known as Data Erasure) this entitles the data subject to request that the data controller erase their personal.

**Data Minimisation** – this means that you can only collect personal data if it's needed to achieve the intended purpose. Personal data should be adequate, relevant and limited to what is necessary.
Where appropriate, such data should also be kept up to date.

**Data Processor** – 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. 'Processing' means any operation, or set of operations, which is performed on personal data or on sets of personal data. It is considered processing whether these operations occur by automated or manual means. Processing includes the following activities: collecting, recording, organising, using, structuring, storing, adapting, retrieving, consulting, destroying and more. The data processor can be an organisation or third-party provider who manages and processes personal data on behalf of the controller. Data processors have specific legal obligations, such as maintaining personal records, and are liable in the event of a data breach.

**Data Protection Officer or named individual responsible for Data Protection** – an appointed individual who works to ensure you implement and comply with the policies and procedures set by UK-GDPR. For Spurgeons the Head of IT & Systems is the responsible person to contact regarding Data Protection.

**Data register –** this is a register that logs the type of personal data and how it is currently being stored and processed.

**Data Subject** – someone whose personal data is processed by a controller or processor.

**Data Subject Rights** – the data subject has the right to:

1. Transparency (to be informed).
2. Access the data.
3. Rectify the data.
4. Request that the data be erased.
5. Restrict processing.
6. Data portability.
7. Object to the processing of data.
8. Not to be subject to a decision based solely on automated processing.

**Encrypted** – personal data which has been translated into another form or code so that only people with specific access can read it.

**Legal Processing** – for any personal data processed, the organisation must be able to specify that it has been processed on one of the legal grounds specified by UK-GDPR. These grounds are:

1. Individuals consent.
2. Contract with the individual (including pre-contract arrangements).
3. Complying with a legal obligation.
4. If it is in the vital interest of the data subject.
5. Necessary for a task in public interest or authority.
6. Necessary in the legitimate interest of an organisation or third party (balanced against interests of the data subject).

**Personal Data** – any direct or indirect information relating to an identified person that could be used as a means of identifying them. This includes their name, ID number, location data or an online identifier, photograph.

**Profiling** – the automated processing of personal data.

**Processing** – this refers to any activity relating to personal data, from initial collection through to the final destruction. It includes the organising, altering, consulting, using, disclosing, combining and holding of data, either electronically or manually.

**Pseudonymisation** – the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately.

**Purpose Limitation** – this refers to using information only for the specified, explicit and legitimate purposes for which the data was collected and not for any other purpose.

**Special Category Personal Data** – more sensitive information relating to a data subject. Includes information which reveals a person's: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

**Third Party** – a legal body or authority other than the data subject, controller or processor who is authorised to process personal data under authority of the data controller or processor.