Data Protection Policy and Statement

1) **Introduction**

Globe Fit is required to keep certain information about its staff, service users and other members of the public to enable it to monitor performance and achievements. It is also necessary to process information so that staff can be recruited and paid, activities organized and legal obligations to funding bodies and government fulfilled.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Globe Fit must comply with the Data Protection Act 1998. In summary this states that personal data must be:

- Obtained and processed fairly and lawfully
- Obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose
- Adequate, relevant and not excessive for that purpose
- Accurate and kept up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to a country Personal data that does not have reciprocal arrangements to the UK, unless that country has equivalent levels of protection for personal data

All Globe Fit staff who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Globe Fit has adopted this Data Protection Policy.

Any member of staff, who considers that this policy has not been followed in respect of personal data about him/herself, should raise the matter with the Designated Data Controller. If the matter is not resolved it should be raised as a formal grievance.

2) **Notification of Data Held and Processed**

All staff, clients and other members of the public have the right to:

- Know what information Globe Fit holds and processes about them
- Know how to request access to it
- Know how to keep it up-to-date
- Know what Globe Fit is doing to comply with its obligations under the Act

3) The Data Controller and the Designated Data Controllers

Globe Fit is the Data Controller under the Act, and the organisation is therefore ultimately responsible for implementation. However, the Designated Data Controller will deal with day to day matters.

4) Information Held

Personal information is defined as any details relating to a living, identifiable individual. This applies to staff, service users and other members of the public. Globe Fit must ensure that information relating to these people is treated correctly and with the appropriate degree of confidentiality.

Globe Fit holds personal information in respect of its staff, service users and other members of the public. This information may include an individual's name, postal, email and other addresses, telephone and facsimile numbers, subscription details, organisational roles and membership status.

Personal information is kept in order to enable Globe Fit to understand the history and activities of individuals or organisations within the voluntary and community sector and to deliver services to its members and service users effectively.

Some personal information is defined as Sensitive Data and needs to be handled with special care.

5) Processing of Personal Information

All staff who process or use any personal information are responsible for ensuring that:

- **a)** Any personal information which is held is kept securely; and
- **b)** Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party

Staff and volunteers should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct.

Personal information should be:

- **c)** Stored in a secure manner
- **d)** If the information is computerised, should be password protected and only accessed by authorised staff
- **e)** If personal information is collected by telephone, callers should be advised what the information will be used for and what their rights are according to the Act.
- **f)** Personal or confidential information should not be discussed in public areas or within open-plan office areas.
- **g)** All staff should be aware of the difficulties of ensuring confidentiality in an open plan area and respect the confidential nature of any information inadvertently overhead.

Any notes taken during or after an interview should be relevant and appropriate. It is recommended that such notes should be filed in a legible and coherent manner and that

information notes are retained for a short period (1 year) in a secure place, before being shredded.

6) Collecting Information

Whenever information is collected about people, they should be informed why the information is collected, who will be able to access it and for what purposes it will be shared. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of Globe Fit.

7) Publication and Use of Globe Fit's Information

Globe Fit aims to make as much information public as is legally possible. In particular information about Globe Fit's staff used in the following circumstances:

- **a)** Globe Fit may obtain, hold, process, use and disclose information in connection with the administration, management and business activities of Globe Fit, including making and keeping lists of members and other relevant organisations
- **b)** Names of, and a means of contacting Globe Fit, will be published within publicity leaflets and on the website

8) Sensitive Information

Sensitive information is defined by the Act as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment purposes or to protect the vital interests of the person or a third party.

9) Disposal of Confidential Material

Sensitive material should be shredded. Particular care should be taken to effectively delete information from computer hard drives if a machine is to be disposed of or passed onto another member of staff.

10) Staff Responsibilities

All staff are responsible for checking that any information they provide to Globe Fit in connection with their employment, is accurate and up-to-date. Staff have the right to request any personal information that is being kept about them either on computer or in manual filing systems by contacting their line manager.

Staff should be aware of and follow this policy, seeking further guidance where necessary.

11) Duty to Disclose Information

There is a legal duty to disclose certain information, namely information about:

- **a)** Child abuse, which will be disclosed to relevant agencies/police
- **b)** Drug trafficking, money laundering or acts of terrorism or treason, serious assault, murder, which will be disclosed to the police.

12) Retention of Data

Globe Fit will keep some forms of information for longer than others. Information about clients cannot be kept indefinitely, unless there are specific requests to do so. General information about clients will be kept for a minimum of 3 years after they have used services, unless required to do so by other statutory bodies.

Globe Fit will also need to retain information about staff. In general, all information will be kept for six years after a member of staff leaves the organisation. Some information however, will be kept for much longer, for example, if required by funders. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment and information required for job references.

A statement about Data Protection will be displayed on the website.

Data Protection Officer
HANNAH MURPHY
07796936041
hannah@globefit.co.uk

DATA PROTECTION STATEMENT

Sharing Information with others

- Sometimes we have to confirm or share information with other organisations. If we need to do this, we will make it clear to you on the forms you complete
- We will draw up an agreement with the organisation that we need to share information when appropriate. This is to ensure that both parties understand why the information is being passed on and what use can be made of it. In some cases, a third-party organisation such as a funding body may draw up the agreement.

Information quality

- We will ensure that the information about you is accurate and up-to-date when we collect or use it. You can help us with this by keeping us informed of any changes to the information we hold about you.

Information security

- We will keep information about you in a secure manner
- We will protect your information against unauthorised change, damage, loss or theft

Keeping information

- We will hold information about you only for as long as the law says. After this it will be disposed of securely and properly

Openness

- We will tell you on request what kinds of information we hold and what we do with it.

Access and correctness

- Whenever possible, we will let you see the information we hold about you and correct it if it is wrong

In general

- We will comply with the Data Protection Act 1998 and any subsequent legislation on information handling and privacy
- We will do this through the Globe Fit's Data Protection Policy and we will help you with any questions or problems that you may have
- If we cannot help you, we will give you advice on where you can access the relevant information

Our Commitment

- We will only collect information that is necessary
- We will be fair in the way we collect information about you
- We will tell you who we are and what we intend to do with the information about you
- Where practicable, we will collect information directly from you
- If we collect information about you from someone else, we will make sure you know that we have done this, whenever possible.

Privacy Policy

1) Introduction

We are committed to protecting your personal information and being transparent about what information we hold about you. Using personal information allows us to develop a better understanding of our patrons and in turn to provide you with relevant and timely information about the work that we do. The purpose of this policy is to give you a clear explanation about how we collect and use the information collected from you directly and from third parties. We use your information in accordance with all applicable laws concerning the protection of personal information (which includes, from 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) and all related data protection legislation having effect in the United Kingdom from time to time) and are responsible as 'controller' of that personal information for the purpose of those laws ("Data Protections Laws").

This policy explains:

- What information we may collect about you;
- How we may use that information:
- In what situations we may disclose your details to third parties;
- Information about how we keep your personal information secure, how we maintain it for and your rights to be able to access it.

If you have any queries about this policy, please contact the Data Protection Officer, Hannah Murphy.

2) Information collection

We collect various types of information and in a number of ways. We collect personal data in relation to our staff, service users and other members of the public to enable it to provide services and activities. Parental consent is sought in relation to any young person participating.

3) Sensitive personal data

The Data Protection Laws recognise that certain categories of personal information are more sensitive such as health information, race, religious beliefs and political opinions. We do not usually collect this type of information about our patrons and other third parties unless there is a clear reason for doing so. For example, we ask for access requirements from audience members so that provision can be made. We also collect health information about our participants in our class, workshops and events so that we have details in case of ill health or emergency whilst participating in activity.

4) Legal basis

There are three bases under which we may process your data:

a) Contract purposes:
When you make a purchase from us or apply to participate in our events you are entering into a contract with us. In order to perform this contract, we need to process and store your data. For example, we may need to contact you by email or telephone in the case of cancellation, or in the case of problems with your payment. We will also process and store your data if you have entered into a contract with the organisation as a third party.

b) Legitimate organisational interests:
In certain situations, we collect and process your personal data for purposes that are in our legitimate organisational interests. However, we only do this if there is no overriding prejudice to you by using your personal information in this way. We describe below all situations where we may use this basis for processing.

c) With your explicit consent:
For any situations where the two bases above are not appropriate, we will instead ask for your explicit consent before using your personal information in that specific situation.

5) Marketing communications

We aim to communicate with you about the work we do in ways that you find relevant, timely and respectful. To do this we use data that we have stored about you, such as what events you have booked for in the past, as well as any preferences you may have told us about. We use our legitimate organisational interest as the legal basis for communications by email.

In the case of email, we will give you an opportunity to opt out of receiving them the first time you create your account with us. If you do not opt out, we will provide you with an option to unsubscribe in every email that we subsequently send you, or you can alternatively use the contact details at the end of this policy.

6) Other processing activities

In addition to marketing communications, we also process personal information in the following ways that are within our legitimate organisational interests:

a) To allow us to improve our services;

b) We may analyse data we hold about you to ensure that the content and timing of communications that we send you are as relevant to you as possible. We may analyse data we hold about you in order to identify and prevent fraud;
c) We may take photos and/or film shows and other events which you attend and use these for promotional purposes. We will however seek express consent for any photos/filming from participants.

In all of the above cases we will always keep your rights and interests at the forefront to ensure they are not overridden by your own interests or fundamental rights and freedoms. You have the right to object to any of this processing at any time. If you wish to do this, please use the contact details at the end of this policy. Please bear in mind that if you object this may affect our ability to carry out tasks above that are for your benefit.

7) Third parties

There are certain circumstances under which we may disclose your personal information to third parties. These are as follows:

a) To our own service providers who process data on our behalf and on our instructions. In these cases, we require that these third parties comply strictly with our instructions and with Data Protection Laws, for example around security of personal data.
b) Where we are under a duty to disclose your personal information in order to comply with any regulatory or legal obligation. This includes when there is a safeguarding risk. See Safeguarding Policy for more details.
c) We may share anonymised, pseudonymised and non-personal information with funders.
d) To the best of our knowledge, understanding and belief your personal information will not otherwise be transferred outside of the EEA or to any country not approved by the European Commission.

8) Website links

Our website, may from time to time, contain links to and from partners', advertisers', affiliates' and social network sites. If you follow a link to any of these websites, please note that these sites have their own privacy policies and that we do not accept responsibility or liability for those policies. Please check those privacy policies before you submit any personal data to those websites as they may not be on the same terms as ours.

9) Maintaining your personal information

Participant personal data is generally stored for 3 years. If we have a legitimate organisational interest in holding such data for a longer period of time then we will do so, however no data is kept for any longer than is reasonably necessary and always subject to the principle of data minimisation.

If there are aspects of your record that are inaccurate or that you would like to remove please use the contact details at the end of this policy. Any objections you make to any processing of

your data will be stored against your record on our system so that we can comply with your requests.

10) Security of your personal information

We have appropriate security measures in place to prevent personal information from being accidentally lost or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your personal information will do so only in an authorised manner and are subject to a duty of confidentiality.

We will always store your digital information on secure servers. Unfortunately, however, the transmission of information via the internet is not completely secure. Although we will do our best to protect your information, we cannot guarantee the security of your information transmitted to our website or otherwise to our servers (such as by email). Any such transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

11) Your rights to your personal information

Under the Data Protection Laws, you have a number of important rights free of charge. In summary, those include rights to:

- Fair processing of information and transparency over how we use your use personal information;
- Access to your personal information and to certain other supplementary information that this Privacy Policy is already designed to address;
- Require us to correct any mistakes in your information which we hold;
- Require the erasure of personal information concerning you in certain situations;
- Receive the personal information concerning you which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to a third party in certain situations;
- Object at any time to processing of personal information concerning you for direct marketing;
- Object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you;
- Object in certain other situations to our continued processing of your personal information; and otherwise restrict our processing of your personal information in certain circumstances.

For further information on each of those rights, including the circumstances in which they apply, see the Guidance from the UK Information Commissioner's Office (ICO) on individuals rights under the General Data Protection Regulation.

If you would like to exercise any of those rights, please:

a) Email Hannah Murphy, our Data Protection Officer
b) Let us have enough information to identify you;
c) Let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and
d) Let us know the information to which your request relates. If you would like to unsubscribe from any marketing emails you can also click on the ‘unsubscribe’ button at the bottom of the email.

12) How to complain

We hope that our Data Protection Officer can resolve any query or concern you raise about our use of your information. You may also use our complaints procedure.

The Data Protection Laws also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner who may be contacted at https://ico.org.uk/concerns/ or telephone: 0303 123 1113.

Please contact our Data Protection Officer - Hannah Murphy if you have any questions about this Privacy Policy or the information we hold about you. If you wish to contact our Data Protection Officer, please send an email to hannah@globefit.co.uk

We are committed to reviewing our privacy policy annually.

This policy was adopted on
Date: 21/02/2024

To be reviewed: 21/02/2025

Signed: Hannah Murphy

GDPR DEFINITIONS & GLOSSARY

- **Accountability**
  GDPR stipulates that organisations must be able to show evidence of their compliance with data protection laws. Accountability is the capacity of organisations to show that they are carrying out measures demanded by the regulations.
  Accuracy Principle
  The notion that data controllers should keep personal data up to date and accurate, taking reasonable steps to ensure that inaccurate data is corrected.
  Anonymous Data
  Data that cannot be traced back to an identifiable individual, and hence falls outside the scope of the GDPR.
  Article 29 Working Party
  A non-regulatory EU-level data protection body that provided advice on how to comply with data protection law to the Member States before the introduction of GDPR. The organisation comprised members of national data protection authorities at the EDPS. It is now the EDPB under GDPR.
  Binding Corporate Rules
  Legally enforceable rules that enable a multinational company or organisation to transfer personal data from its entities in the EU to its entities (subsidiaries and affiliates but not third parties) in countries outside the EEA.
  Biometric Data
  Biometric data refers to any data derived from a data subject's biology or physical body. These data could include information regarding the physiological, behavioural or physical characteristics of a natural person, including iris scans, fingerprints, and facial images.
  Breach
  A security failure that leads to the accidental or unlawful access, disclosure, loss or destruction of personal data.
  Breach Notification
  The requirement for organisations to report data breach to the supervisory authority (ICO in the UK) within 72 hours of becoming aware of the breach. The individual data subjects impacted in the breach may also need to be notified in case of a risk to their rights or freedoms.
  Consent
  Any act by the owner of data that indicates that they are willing to allow their data to be processed for a specific purpose. Consent must be unambiguous, informed, specific and freely given and can be retracted by the data subject at any time under GDPR.
  Cross-Border Processing
  Any situation in which the data processor or data controller operates across multiple Member States and processes personal information across those borders. Cross-border processing also refers to a situation in which a data controller operates in one country, but receives data from data subjects in multiple countries.
  Data Controller

The controller (organisation or individual) the main decision-makers in relation to personal data. They exercise overall control over the purposes and means of the processing of personal data. Employers are data controllers of their employees' data. Joint controllers are two or more controllers that jointly determine the purposes and means of the processing of the same personal data.

Data Portability

Data portability is a scheme that makes it easier for individuals to transfer their data from one controller to another. GPDR gives data subjects the right to receive their data in electronic format and then pass it on to another controller (for example, if they want to change service provider).

Data Privacy Impact Assessment (DPIA)

A DPIA is a process that is used to help identify and minimise the data protection breach risks that come with processing any personal information. When it comes to processing, there are certain types that require a DPIA. This is usually the case when any type of processing is considered to be high risk in terms of security leaks.

- Describes the data processing in place and purpose for doing it
- Assesses whether the processing is necessary
- Identifies and assesses the risk to data subjects
- Determines any measures that can be put in place to mitigate risk and help to protect data from breaches.

Data Processing

In the context of data protection, processing covers a wide range of manual or automated operations performed on personal data, including the collection, recording, structuring, storage, adaptation or alteration, archival, retrieval, consultation, use, disclosure by transmission, dissemination or publishing, combination, restriction, and erasure or destruction of personal data.

Data Processing Agreement (DPA)

A legally binding contract (required under GDPR Article 28 Section 3) that states the rights and obligations of the data processor and data controller concerning the protection of personal data.

Data Processor

Any individual or organisation with authorisation to edit, modify, delete, transfer, use or change a data subject's personal data. A data controller can be the data processors too, or may outsource processing to a third party (which then is the data processor).

Data Protection Act (DPA)

The Data Protection Act 2018 sets out the data protection framework in the UK, alongside the GDPR.

Data Protection Authority

Each member state of the EU has a data protection authority or supervisory authority. The job of the national DPA is to ensure that member states of the EU enforce data protection law. Many DPAs have extensive enforcement powers, allowing them to impose fines on organisations and individuals who do not comply. The authority in the UK with these powers is the ICO.

Data Protection Officer (DPO)

A data protection officer is a person who works in an organisation to ensure that the business complies with data protection laws. Not all organisations have DPOs, but some have to by law, especially those who process special categories of data. The DPO is responsible for monitoring data protection compliance, keeping you informed about our data protection obligations, and providing any necessary advice for remaining compliant at all times.

Data Protection Principles

Seven key principles set out by the GDPR that should lie at the heart of any approach to processing personal data: Lawfulness, fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality (security), Accountability.

Data Security

Data security is the term used for how digital data is protected from the unwanted actions of unauthorized users, including cyber-attacks and data breaches.

Data Subject

A data subject is any person to whom data can be attributed and, thus, falls under the jurisdiction of existing data protection laws. Subjects could include a customer, employee, a third-party contact or any individual with whom a data controller interacts.

DPA 2018

Data Protection Act 2018

EDPS

The EDPS or European Data Protection supervisor is an EU-level public body that ensures that institutions within the EU respect EU citizen's right to privacy and data protection while processing their data. The body is made up of representatives from member state national data protection institutions.

Encryption

Encryption is a mathematical operation to encodes data in such a way that it can only be accessed by authorised users. Article 32 of the GDPR includes encryption as an example of an appropriate technical measure.

Fairness Principle

A principle which states that a data controller should put in place facilities that enable the data subject to exercise rights pertaining to their data. Under the fairness principle, data controllers could include facilities that provide access, rectification and erasure of the data as well as those that allow the subject to place restrictions on processing or transfer the data from one controller to another.

GDPR

The General Data Protection Regulations (GDPR) is an EU law that concerns the privacy and data protection of all citizens in the EU and the European Economic Area (EEA).

Genetic Data

Any data that describes the biological characteristics of a subject at the level of DNA. Genetic information, for instance, could include a person's entire genome, their genetic markers, DNA information that can identify them, or information related to their characteristics or disease status.

Information Commissioner's Office (ICO)

The Information Commissioner's Office is the supervisory authority under the data protection laws in the UK. It is non-departmental body that reports directly to the UK parliament. Data

controllers and data processors in the UK need to register with the ICO and need to notify data breaches to the ICO.

Legality Principle

A legal paradigm that states that organisations should only use personal data on the grounds specified by GDPR. The legitimate use of data includes situations in which an individual gives their consent, there is a contract with the individual, or using data allows the organisation to comply with an existing legal obligation.

Member States

Countries that are part of the European Economic Area (or European Union) and subject to GDPR.

Minimisation Principle

Data processors should keep as little information on data subjects as possible and only collect data that they require for their processing. They should not seek out additional data that is not necessary for them to carry out their objectives.

Natural Person

A natural person refers to an entity under the law classified as a human being. A non-natural person under the law could refer to an organisation, public or private, sometimes called a legal person.

One-Stop-Shop

Many businesses have locations across a number of EU Member States. The One-Stop-Shop concept allows companies to deal with the lead GDPR regulator in their home country, not all regulators in all countries in which they operate.

Parental Consent

In the UK, only children aged 13 or over are able provide their own consent for processing their personal data. Under this age, it is necessary to obtain consent from whoever holds parental responsibility for them.

Personal Data

Personal data includes any data that a third-party could use to verify the identity of the data subject - the person to whom the data refers. It could consist of bank details, phone, numbers, addresses, names, photos or data gleaned from social networks.

Personal Data Breach

An event in which a subject's data is somehow lost, stored, disclosed or transmitted in a way that contravenes the GDPR. Personal data breaches can be either accidental or deliberate.

Principles of Data Protection

A set of basic statements describing the spirit and purpose of the GDPR. The principles also set out the main objectives of the regulations and the mission of the public bodies that will enforce them across the EU.

Privacy by Design

A concept whereby organisations build privacy into their processes from the outset, reducing the likelihood of a data breach in the future. Privacy by design, for instance, could involve the development of technical systems that better protect subject data compared to existing protocols ahead of time, rather than waiting for a data breach to make changes.

Privacy Impact Statement

GDPR rules state that data controllers must create a privacy impact statement (also called a

Data Protection Impact Assessment) whenever processing data that might present a privacy risk. Data processing could be a privacy risk because of its purposes, scope or nature.

Privacy Notice

A privacy notice is a document in which a data controller tells people what they'll be doing with their personal data and whom they'll share it with, etc.

Privacy Shield

The EU-US Privacy Shield is a scheme that is deemed by the European Commission to provides adequate protection to allow personal data to be transferred to entities in the United States that are registered under this scheme.
Visit the privacy shield website to verify if an organisation is registered.

Processing

See Data Processing.

Profiling

Profiling is a tool that attempts to use patterns in data to discern secondary information about a subject. Companies often use profiling to analyse employee behaviour, preferences or capacity to perform reliably at work.

Pseudonymisation

A process that permits the processing of data such that the contents can no longer be traced back to the original data subject without the use of additional information. Organisations and data controllers who use pseudonymisation often keep identifiable and non-identifiable data separately.

Purpose Limitation Principle

Data processors should only collect data for explicit, legitimate reasons and not use it in further ways that are not compatible with the initial purpose.

Rectification

The correction and/or completion of inaccurate or incomplete data.

Regulation (EU) 2016/679

The official regulation code for the EU General Data Protection Regulation (GDPR) approved by the European Parliament and Council on April 27, 2016. GDPR applies to member states without the need for national legislation implementation.

Restricted Transfers

GDPR puts in place restrictions for any organisation wanting to transfer data outside of the EEA. The rules define transfer as both the physical transportation of data outside of the EEA, but also remote viewing of EU data subjects' data by international third parties, eg by digital means.

Restriction on Processing

The act of marking stored data to prevent the further use or processing of that data in the future. A data controller, for instance, might restrict processing, if he or she believes that further use of the data might put the privacy of the owner at risk.

Right to Access

Data subjects have the right to access all the data that we hold on them. Such a request is called a Subject Access Request (SAR). It can be given to us verbally or in writing on paper or any online channel.

Right to be Forgotten

See Right to Erasure.

Right to be Informed
Data subjects have the right to be informed about the purpose for which we are holding and processing their personal data. This is typically done with a privacy notice.
Right to Data Portability
Data subjects have the right to data portability - ie to obtain a copy of their data in a standard format, even if they are moving it to one of our competitors.
Right to Erasure
Data subjects have the right to the erasure of their data (also known as the right to be forgotten) unless we have a legitimate interest to hold the data.
Right to Object
If the data subject doesn't want their data to be used for a certain purpose - e.g. profiling - they have the right to object.
Right to Rectification
Data subjects have the right to rectification of any inaccurate or incomplete data.
Right to Restrict Processing
In addition to the right to erasure, data subjects also have the right to restrict processing, whereby we may store the data but have to refrain from processing it.
Rights on Automated Decision Making & Profiling
Data subjects also have rights with respect to automated decision making and profiling.
Sensitive Personal Data
Any form of personal data that the GDPR consider uniquely special or sensitive. These data include information relating to religious affiliation, sexual orientation, ethnic and racial origins, trade union membership, and biometric/DNA data that could identify a person.
Special Category Data
See Sensitive Personal Data.
Storage Limitation Principle
The storage limitation principle states that data controllers must only retain information for as long as they need it for processing purposes. Data controllers should not keep personal data for longer than is necessary. Long-term storage is only permitted for public interest archiving or statistical research purposes.
Subject Access
GDPR rules state that subjects have the right to access their personal data held by a data controller. A subject can request a data controller to give them access to any personal data that they hold.
Subject Access Request (SAR)
A subject access request is a request for access made by the data subject. The GDPR does not specify how to make a valid request. Therefore, it could be verbal or in writing. It can be made to any part of the organisation - it does not have to be to a specific person or contact point. It doesn't even need to formally say 'subject access request'. As long as it is clear that the individual is asking for their own personal data, the organisation needs to recognise it as a SAR and respond to it within one month. Unless the request is manifestly unfounded or excessive or repetitive, the organisation cannot charge a fee.
Supervisory Authority
See Data Protection Authority or ICO in the UK

Territorial Scope
The term territorial scope refers to the geographic region over which the EU GDPR rules apply. Currently, GDPR encompasses the European Economic Area (EEA), which includes all current 28 EU member states. It also covers additional territories, including Norway, Lichtenstein and Iceland. It does not include Switzerland.

Third Party
In the context of GDPR, a third party is any person who legitimately interacts with protected data and is neither a data subject nor a data controller. Third parties receive authorisation to process or view data from either the data controller or the data subject.

Transparency Principle
The notion that data controllers should give data subjects data on request that is accessible, understandable, intelligible and provided in written form. Thus, data subjects should be able to understand the data the organisations or data controllers have about them and be able to make requests based on those data.

Vulnerable Customers
Customers who are more vulnerable than others, for example, due to their state of mental capacity, or having been diagnosed with a terminal illness. The category and level of data that a firm could now hold on a customer, could far exceed their original expectations and be far more reaching into the personal life of the customer than they initially had established data storage and retention controls for.