Data Protection Policy

Version 3 — September 2026

1. Introduction 4
   1.1. What is GDPR? 4
   1.2. What Firms does GDPR apply to? 4
   1.3. Territorial Scope 4
2. GDPR Principles 4
3. What is Personal Data? 6
   3.1. Personal Data 6
   3.2. 'Special Category' Personal Data 6
   3.3. Criminal Offence Data 7
4. Lawful basis for processing data 7
   4.1. Processing must be 'necessary' 7
   4.2. Deciding upon which lawful basis to apply 7
   4.3. The Six Lawful Bases 8
   4.4. When must we decide on our lawful basis 9
   4.5. What happens if we have a new purpose 9
   4.6. Documenting our lawful basis 9
   4.7. Disclosing our lawful basis 9
   4.8. Processing Special Category Personal Data 9
   4.9. Processing Criminal Offence Data 10
5. Transfer of Data (outside the UK) 10
   5.1. 'Adequacy' 10
   5.2. Appropriate Safeguards 11
   5.3. Derogations from the transfer of data requirements 11
   5.4. One-off/Infrequent transfers/small number of data subjects 12
6. Data Subject Rights 12
   6.1. The right to be informed 12
   6.2. The right of access 13

6.3. The right to rectification..... 13
6.4. The right to erasure..... 13
6.5. The right to restrict processing..... 13
6.6. The right to data portability..... 13
6.7. The right to object..... 14
6.8. Rights in relation to automated decision-making and profiling.....
7. Data Protection Officer..... 14
8. Data Protection Fee..... 14
9. IT security..... 15
9.1. Physical Security – Factors to consider..... 16
10. Requirements on Data Processors?..... 17
11. Staff Training..... 17
12. Record keeping..... 18
12.1. Data Retention periods..... 18

1. Introduction

1.1. What is GDPR?

The UK GDPR, retained under the European Union (Withdrawal) Act 2018, took effect on 1 January 2021. The original EU GDPR took effect on 25th July 2026 and updated the Data Protection Act to reflect changes in technology and data use. It places greater emphasis on documenting data protection procedures, accountability and governance arrangements, and on how organisations manage data protection as a corporate issue. Following Brexit, the UK retained the GDPR as the UK GDPR. It is directly binding on the United Kingdom. The GDPR is regulated and enforced in the UK by the Information Commissioner's Office ("ICO"), but the FCA will consider compliance with the GDPR when determining whether a Firm is operating in accordance with the FCA's Senior Management Arrangements, Systems and Controls ("SYSC") rules. The FCA has stated that, in the context of the GDPR and as part of their obligations under SYSC, Firms should establish, maintain and improve appropriate technology and cyber resilience systems and controls.

1.2. Other Legislation

The Data (Use and Access) Act 2025 (DUAA) was introduced to update and refine the UK's data protection framework following the UK's departure from the European Union. Building on the UK GDPR and the Data Protection Act 2018, the Act aims to support responsible data use, innovation, and economic growth while upholding high standards of personal data protection.

The Firm recognises that the UK data protection framework continues to evolve, including through the DUAA. The Firm will adopt a proportionate, risk-based approach to data protection, ensuring its practices comply with current legal requirements and remain adaptable to future legislative developments.

1.3. What Firms does GDPR apply to?

GDPR applies to firms that fall within the definitions of 'data controllers' and 'data processors' as set out below:

- A controller is: '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**'
- A processor is: 'a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**'

SCM Private LLP ("SCM") is a discretionary fund manager and therefore a data controller, as we determine the purpose and means of processing the personal data we hold on behalf of our clients. We also hold personal data relating to our employees. We may involve a processor to assist us with the data we hold, but we ensure that such relationships are governed by GDPR-compliant contracts.

1.4. Territorial Scope

The UK GDPR applies to organisations operating in the UK and to those outside the UK that process the personal data of UK data subjects. Post-Brexit, the UK operates its own data protection regime under the UK GDPR and the Data Protection Act 2018.

2. GDPR Principles

Article 5 of the GDPR sets out the key principles that personal data must be processed in accordance with:

1. **Lawfulness, Fairness and Transparency.** Personal data must be processed lawfully, fairly and in a transparent manner. Under this principle, we will always tell data subjects what processing will take place (transparency). Processing must always match the description given to the data subject in a notice (fairness), and it must always be for a purpose specified in the GDPR (lawfulness).

2. **Purpose Limitation.** Personal data must be collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes. Under this principle, firms should always inform data subjects how they will use their personal data.

3. **Data Minimisation.** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy.** Personal data must be accurate and kept up to date. We must establish appropriate processes for identifying and addressing out-of-date, incorrect or redundant personal data.

5. **Storage Limitation.** Personal data must be kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which they are processed. We should adopt technical and organisational measures to store personal data by pseudonymising it, wherever possible, or disposing of it once the purpose for processing is met, where no further legitimate conditions for data retention apply.

6. **Integrity and Confidentiality.** Personal data must be processed in a way that ensures protection against unauthorised or unlawful processing, accidental loss, destruction or damage. These measures include, but are not limited to, encryption, restrictions to rights of access to personal data, appropriate instructions and training to employees on how to process personal data, and physical security measures to access areas where paper-based personal data are stored.

We have in place the following policies and procedures to demonstrate that we have systems and controls to comply with the above Principles:

- Data Protection Policy
- Completed ICO GDPR Documentation Controller Template
- Data Breach Policy
- Privacy Notices (for Staff and clients/investors whose personal data we hold).

Our procedures are as follows:

- All staff must read this policy to ensure they have a basic understanding of GDPR
- The Compliance Officer is the main point of contact for data protection at the Firm.
- The Compliance Officer is responsible for updating/maintaining the data protection record-keeping
- All Subject Access Requests must be forwarded to the Compliance Officer

- All data breaches must be notified to the Compliance Officer
- Privacy Notices are sent to all clients (upon take-on) and staff (upon joining)
- Any transfers of data outside of the UK must be pre-notified to the Compliance Officer
- Annual regulatory/financial crime training includes an overview of GDPR

3. What is Personal Data?

3.1. Personal Data

GDPR applies to 'personal data', meaning any information that, directly or indirectly, allows identification of a living natural person by reference to an identifier. It is defined broadly and includes information such as:

- Name
- Date of birth
- Address/location identifiers
- Photos & CCTV images
- Online identifiers (such as IP address)
- Identification number(s) (such as client reference numbers, passport numbers, bank account details, credit card numbers, national insurance numbers, etc)

Key-coded/'pseudonymised' data may also be personal data depending on how easy it is to attribute it to a specific person.

The requirements in relation to personal data apply to both automated personal data and manual filing systems where personal data are accessible according to specific criteria.

3.2. 'Special Category' Personal Data

This refers to sensitive data that requires greater protection due to its private or potentially intrusive nature. In addition to requiring one of the 6 lawful bases for processing, organisations that process 'special category' data must also meet one of the additional conditions for processing special category data under Art 9 of the GDPR. Special category data includes information relating to an individual:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)

- Health
- Sex life
- Sexual orientation

There are additional requirements to process 'special category' data (at Art 9(2)) which are, in summary:

a) The data subject has given explicit consent

b) Processing is necessary to carry out the specific rights of the controller or of the data subject in relation to employment and social security and social protection law

c) Processing is necessary to protect the vital interests of the data subject

d) Processing is carried out during legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body in relation to present or past members or certain connected persons of that body and is not disclosed outside that body.

e) Processing relates to personal data which is manifestly made public by the data subject

f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in a judicial capacity.

g) Processing is necessary for reasons of substantial public interest

h) Processing is necessary for the purposes of preventative or occupational medicine

i) Processing is necessary for reasons of public health e.g. protecting against serious cross-border threats to health or ensuring safety of health care or medical products

j) Processing is necessary for archiving purposes in the public interest, scientific or historical research, or statistical purposes.

3.3. Criminal Offence Data

The processing of criminal conviction and offence data ("Criminal Offence Data") is similar to Special Category Data but requires greater protection due to its private or potentially intrusive nature.

For example, details of criminal convictions uncovered about staff, typically gathered during pre-employment screening, will be Criminal Offence Data.

We must not keep any comprehensive register of criminal convictions unless we do so under the control of an official authority.

There are additional requirements to process 'criminal offence' data as set out in section 4.

4. Lawful basis for processing data

4.1. Processing must be 'necessary'

Many of the lawful bases set out below depend on the processing being "necessary". This does not mean that processing must always be essential; however, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other, less intrusive means.

4.2. Deciding upon which lawful basis to apply

We should consider which lawful basis best fits the circumstances, considering our specific purposes and the context of the data processing. Where more than one basis applies, we will identify and document each at the outset.

No basis should be considered better, safer or more important than the others. The Firm recognises that UK data protection law permits a degree of flexibility in determining the lawful basis, particularly where processing is necessary and proportionate to achieve a legitimate purpose.

In deciding which basis best fits our circumstances, we should consider a variety of factors, including:

- What is our purpose – what are we trying to achieve?
- Can we reasonably achieve it in a different way?
- Do we have a choice over whether to process the data?

Contractual basis - Where there exists a contractual basis for processing personal data, for example under a client agreement for investment services, then the appropriate lawful basis will be obvious – 'contract'.

If we are processing data for other than contractual purposes, then we are likely to have a choice between relying upon legitimate interests or consent. However, we should consider the wider context, including:

- Would individuals expect this processing to take place?
- What is our relationship with the individual?
- What is the impact of the processing on the individual?
- Is the individual concerned likely to object?
- Are we able to stop the processing at any time on request?

Legitimate interests - We may prefer legitimate interests as our lawful basis if we want to keep control over the processing and take responsibility for demonstrating that it aligns with the individual's reasonable expectations and doesn't have an unwarranted impact on them.

Consent - On the other hand, if we prefer to give individuals full control over and responsibility for their data, including the ability to change their mind as to whether it can continue to be processed, we may want to consider relying on the individuals' consent.

4.3. The Six Lawful Bases

The 6 lawful bases, of which organisations must have at least one, are set out below:

1. **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract that we have with the individual, or because they have asked us to take specific steps before entering into a contract.
3. **Legal obligation:** the processing is necessary for us to comply with legal requirements under UK law (not including contractual obligations as per 2 above).
4. **Vital interests:** the processing is necessary to protect a person's life.
5. **Public task**: the processing is necessary to perform a task in the public interest or for official functions and the task has a clear basis in law. This includes circumstances where the basis for such processing is established in:
    - UK domestic law; or
    - relevant international law, including international agreements or treaties to which the UK is a party.

    Where relying on this lawful basis, the Firm will ensure that:
    - The processing activity is clearly linked to a recognised public interest purpose;
    - The relevant legal basis (domestic or international) is identified and documented; and
    - The processing is necessary and proportionate for the intended purpose.

    Where special category data is processed on public interest grounds, the Firm will ensure that an additional condition under applicable legislation is satisfied.
6. **Legitimate interests**: the processing is necessary for our legitimate interests or the legitimate business interests, provided that such interests are not overridden by the rights and freedoms of the individual. We apply a proportionate and risk-based assessment when relying on legitimate interests, considering the nature, context and impact of the processing activity. We rely on this basis for direct marketing, intra-group data transfers, and for ensuring the security of network and information systems. Where we rely on legitimate interests, we will undertake a Legitimate Interest Assessment to ensure that:
    - The processing is necessary for a clearly defined purpose;
    - The impact on individuals has been considered; and
    - Appropriate safeguards are implemented to protect personal data.
7. **Recognised Legitimate Interest:** We may rely on "recognised legitimate interest" as a lawful basis for processing personal data, where permitted under applicable UK data protection legislation.

    Recognised legitimate interests apply to certain processing activities where the processing is necessary and proportionate for particular purposes. Where these conditions apply, we may not be required to undertake a full balancing test, provided the relevant statutory criteria are met, such as disclosures to public bodies, National Security/Public Security/Defence,

emergency situations, the prevention or detection of crime, and the safeguarding of vulnerable individuals.

There are exemptions from GDPR where processing is performed by a natural person for a purely personal/household purpose and (in certain circumstances) where it is performed by a law enforcement agency or by UK government institutions.

4.4. When must we decide on our lawful basis

We must decide on a lawful basis before becoming the data controller. On an ongoing basis, we can choose a new lawful basis or decide that a different basis is more appropriate. However, switching between lawful bases may be difficult if we find that our original basis was invalid, as we may then be in breach of the GDPR.

4.5. What happens if we have a new purpose

If our purpose for processing data changes over time, or we have a new purpose, we may not need a new lawful basis.

However, this does not apply to processing based on consent, as consent must always be specific and informed. In such circumstances, we would need either to obtain fresh consent that specifically covers the new purpose or to find a different basis for that purpose.

As a rule, if the new purpose is very different from the original purpose, unexpected, or unjustified in its impact on the individual, it is unlikely to be compatible with our original purpose for collecting the data.

Even if processing for a new purpose is lawful, we must also consider whether it is fair and transparent and provide the individual with information about the new purpose.

4.6. Documenting our lawful basis

We must be able to show that we have properly considered which lawful basis applies to each processing purpose and can justify our decision. We therefore must keep a record of which basis we are relying on for each processing purpose, and a justification for why we believe it applies.

4.7. Disclosing our lawful basis

We must disclose to any data subjects which lawful basis we are relying on for processing their personal data. We include this within the Firm's Privacy Notice sent to all individuals and clients.

4.8. Processing Special Category Personal Data

Where we seek to process special category data, we must identify and document both our 'lawful basis' for processing and a 'special category' condition (see section 3.2).

Our choice of lawful basis does not dictate which special category condition we must apply, and vice versa. For example, if we use consent as our lawful basis, we are not restricted to using explicit consent for special category processing.

4.9. Processing Criminal Offence Data

Where we seek to process Criminal Offence Data, which includes data about criminal convictions, criminal offences or related security measures, we must identify and document both our 'lawful basis' for processing and a 'separate condition' for processing this type of data.

5. Transfer of Data outside of the UK

Generally, personal data may be transferred to a third country or international organisation where:

- The destination has been recognised as providing an adequate level of protection; or
- Appropriate safeguards are in place, such as standard contractual clauses or other approved transfer mechanisms; or
- A specific exemption applies under applicable law:

When relying on transfer mechanisms or safeguards, we will assess whether the level of protection afforded to personal data is not materially lower than that provided under UK data protection law.

In carrying out this assessment, we will take a reasonable and proportionate approach, considering the:

- Nature of the data being transferred;
- Purpose and context of the transfer;
- Legal and regulatory environment in the destination country; and
- Safeguards in place to protect the data.

We will ensure that appropriate documentation is maintained to demonstrate that international transfers have been assessed and implemented in compliance with applicable requirements.

We will monitor international data transfers on an ongoing basis to ensure that protections remain appropriate over time.

GDPR requires that certain conditions must be met before personal data can be transferred outside of the UK as follows:

5.1. 'Adequacy'

The transfer of personal data may take place where the UK Government has decided that the third country/territory/specific sector within that third country has an 'adequate level of protection' in terms of the holding and processing of data.

As at the date of this policy, the UK Government recognises the following third country jurisdictions as meeting the adequacy requirements:

- European Economic Area (EU/EEA member states)
- Andorra
- Argentina
- Canada (commercial organisations)

- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- United States (organisations covered by the UK Extension to the EU-US Data Privacy Framework[1])

The UK has also granted adequacy to:

- Japan
- South Korea

The above adequacy decisions do not cover data exchanges where required under Art 36 of the Police Directive.

If we want to transfer data to a third country for which there is no UK Government decision on data protection adequacy, we can do so only if we have ensured that certain 'appropriate safeguards' are in place and that enforceable data subject rights and effective legal remedies for data subjects are available.

5.2. Appropriate Safeguards

We may transfer personal data outside the UK where we believe there will be adequate safeguards, individuals' rights are enforceable and effective legal remedies are available following transfer. Adequate safeguards include:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between Firms within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the ICO or UK Secretary of State;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the ICO;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;

[1] The EU-US Privacy Shield was invalidated by the CJEU in 2020. The UK has since established the UK Extension to the EU-US Data Privacy Framework and its own international data transfer mechanisms including the International Data Transfer Agreement (IDTA). For more information see: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/

- contractual clauses agreed and authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Where data is transferred to an external entity, Firms are most likely to ensure that appropriate safeguards are in place by including a standard clause. Where the Firm relies on third-party service providers such as Administrators, Custodians, and Law Firms, it must ensure that the Third Parties outside the UK have in place sufficient levels of protection that are equivalent to those required by the Act.

Where adequate safeguards cannot be met, the Firm should terminate its contract or ensure that no personal data is being transferred.

5.3. Derogations from the transfer of data requirements

Although not encouraged, there are a number of limited circumstances where Personal Data can be transferred outside of the UK:

1. Consent. Where the Firm can transfer personal data overseas if it has the individual's consent, which should be given clearly and freely and may later be withdrawn by the individual
2. Contract performance. Where it is necessary to perform a contract of services.
3. Substantial Public interest. This is a high threshold, and it is most likely to be relevant in areas such as preventing and detecting crime, national security, and collecting tax.
4. Vital Interest. The Firm can transfer personal data overseas where it is necessary to protect the vital interests of the individual. This relates to matters of life and death.
5. Public Registers. The Firm can transfer overseas part of the personal data on a public register, if the person transferred complies with any restrictions on access to or use of the information in the register.
6. Legal Claims. Where necessary for the execution of legal proceedings
7. Where it is being sent to a country recognised by the UK Secretary of State as offering adequate protection (this would include US organisations that are UK Extensions to the EU-US Data Privacy Framework certified).

Please revert to the Compliance Officer if in any doubt.

5.4. One-off/Infrequent transfers/small number of data subjects

Even where 'adequacy', 'appropriate safeguards', and 'derogations' do not apply, personal data may still be transferred outside the UK. However, such transfers are subject to certain conditions, including the requirement to inform the relevant supervisory authority of the transfer and to provide additional information to individuals (under Art 13 and 14 of the GDPR), including what 'compelling legitimate interests' are being pursued. Transfers of data on this basis are only permitted where it:

- is not being made by a public authority where executing its public powers;
- is not repetitive (similar transfers are not made on a frequent/periodic basis);
- involves data related to only a limited number of individuals;

- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

6. Data Subject Rights

GDPR protects the following 8 rights of individual data subjects:

6.1. The right to be informed

GDPR requires that Firms be specific about how they use the personal data they hold on individuals. We must actively inform those individuals about what information we hold, the basis for processing their data, the types of data held and shared with others (if applicable), and their individual rights.

We will provide individuals with a 'Privacy Notice' that contains the above information (so-called 'privacy information') in a clear and transparent manner. This will be provided to individuals 'within a reasonable period' of obtaining the personal data, and no later than 1 month. The Privacy Notice must be accessible to individuals, and individuals must be made aware of it.

The Firm has separate Privacy Notices (for Staff/contractors and for Clients/website) which are held by the Compliance Officer.

6.2. The right of access

GDPR allows individual data subjects to access their personal data (and supplementary information) so that they are aware of and can verify the lawfulness of the processing.

Where an individual makes a 'subject access request' for personal data, we must provide that information promptly, in a commonly used electronic format, and at the latest within one month of receipt (unless the requests are complex or numerous, in which case it must be provided within a further two months). We can refuse a request where it is manifestly unfounded or excessive, or we may charge a reasonable fee based on the cost of processing the request.

6.3. The right to rectification

Individuals have the right to request the rectification of inaccurate or incomplete personal data, and we have one month to respond. This refers to the accuracy principle, which requires 'every reasonable step to be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.

6.4. The right to erasure

Individuals can exercise their right to have their personal data erased in certain circumstances, for example, where it is no longer necessary for the original purpose for which it was collected, or where the individual objects to their data being held for direct marketing purposes. However, the right to erasure is not absolute. An individual may not have their personal data erased where, for instance, it is necessary to comply with a legal obligation, for the establishment, exercise or defence of legal actions, or where it is in the public interest.

6.5. The right to restrict processing

As with the right to erasure, the right to restrict processing is not an absolute right. Individuals can request that the processing of their personal data be restricted in certain circumstances, for instance, when they believe there are inaccuracies in the data we hold and wish to restrict processing whilst it is verified, or where we no longer need to process the personal data but they wish us to retain it to establish, exercise or defend a legal claim. Processing is 'restricted' where we store the personal data but may not use it. We will take measures to ensure that the data is flagged as restricted or inaccessible to persons who may inadvertently process it. We can only process stored restricted data where the individual consents or where there are applicable legal or public interest reasons for doing so.

6.6. The right to data portability

Individuals may obtain and transfer their personal data from one IT platform/service to another, without undue obstruction, where the data is processed by automated means (e.g., price comparison websites).

6.7. The right to object

Where we process personal data based on 'legitimate interest' (or public interest/official authority), for direct marketing (including profiling), and for scientific research/statistics purposes, the individual has the right to object. We must ensure that our privacy notice explicitly informs individuals of this right, and in any event, 'at the point of first communication'. If we receive an objection in relation to our direct marketing activities, we must cease processing data for this purpose immediately (and, where such marketing takes place online, the Firm must offer an opt-out). We can only continue to process data following an objection if we can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the individual, or if the processing is for the establishment, exercise or defence of legal claims.

6.8. Rights in relation to automated decision making and profiling

There are separate and detailed requirements for where Firms process data in relation to automated individual decision-making and profiling. Firms conducting such activities should refer to the detailed guidance issued by the ICO:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

7. Data Protection Officer

The GDPR introduces specific accountability requirements, including the mandatory appointment of a Data Protection Officer ("DPO") by a data controller or a processor where:

- The processing is carried out by a public authority;
- The core activities of the firm consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or
- The core activities of the firm consist of large-scale processing of special categories of data and data relating to criminal convictions or offences.

When a DPO is not required under the GDPR, a firm should still identify and record who within its organisation is responsible for GDPR compliance.

We have considered this requirement and concluded that the appointment of a DPO is not required for our firm. Responsibility for GDPR compliance is assigned to Alan Miller.

8. Data Protection Fee

Previously, firms deemed to be controllers had to notify or register with the ICO. Under the new regime, there is no requirement to notify the ICO, but controllers must pay the ICO a data protection fee unless they qualify for an exemption. Further details can be found in the ICO publication: "Data protection fee - a guide for controllers".

9. IT security

One of the principles under the GDPR - the 'security principle' - requires that data be processed securely and in line with 'appropriate technical and organisational measures'. This is not a new requirement, as the Data Protection Act already required Firms to have data security measures in place. The key requirement is that Firms must be able to prevent the personal data they hold from being accidentally or deliberately compromised. This applies to (a) cybersecurity (the protection of networks and information systems) and (b) physical and organisational measures.

Where a firm is processing data, it should consider the following factors, proportionately:

Obscuring	Consider whether pseudonymisation and encryption is appropriate (updated ICO guidance on encryption not available yet)
'CIA triad'	Ability to ensure the ongoing '**c**onfidentiality, **i**ntegrity, **a**vailability' of information security. The Firm's IT security measures should guarantee all 3 are met.
Resilience	Are the processing systems and services able to continue operating under adverse conditions, e.g. a physical/technical incident, and can they be restored to a working state?
Security Event	Consider how the Firm would restore the availability and access to personal data in a 'timely manner' if there was a physical/technical incident, e.g. ensure there is a back-up process.
Testing	GDPR requires Firms to test the effectiveness of IT security measures. Frequency and detail of these depends upon the nature and scale of processing.
Code of certification	If your security measures include a product/service that adheres to a GDPR code of Conduct (once approved) or Certification (once issued), this can demonstrate compliance with the Security requirements.

Cybersecurity – Factors to consider.

The ICO's guidance on security suggests that Firms consider the following factors when reviewing IT systems (and whether specialist external advice is required, depending on the sophistication of your systems, usage requirements and staff technical expertise):

System security	Check the security of your network and information systems, including those which process personal data
Data security	Check the security of the data held in the Firm's systems e.g. ensuring appropriate access rights/authorisations and that data is held securely.
Online security	Check the security of your website and any other online service or application you use
Device security	Consider implementing policies on 'Bring-your-own-device' (BYOD) if applicable. Note that this link relates to pre-GDPR guidance on BYOD is currently under review by the ICO (so please check the website for updates). https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

You may wish to consider the requirements of 'Cyber Essentials' (the Government scheme that outlines basic IT security controls that are simple enough for companies to implement themselves). Cyber Essentials provides guidance on five technical controls and implementing them will demonstrate that you are operating at an appropriate (minimum) level of security. In summary, they are:

1. **Use a firewall to secure your internet connection:** A firewall creates a 'buffer zone' between your IT network and external networks whereby incoming traffic can be filtered to determine whether it poses a threat to your network or not.

2. **Choose the most secure settings for your devices and software**: Check the settings on new software and devices to ensure that any default settings (which may present more opportunities for cyber attackers to gain unauthorised access to your data) are changed. Change all default passwords and implement extra security such as two-factor authentication (2FA) where appropriate.

3. **Control who has access to your data and services**: implement access controls for software, settings, online services and device connectivity functions to ensure permissions are appropriate to the functions staff or users are performing.

4. **Protection from viruses and malware**: implement anti-malware systems, consider 'whitelisting' (creating a list of applications allowed on a device whereby unlisted applications are then blocked) and 'sandboxing' (sandboxed applications run in an isolated environment with very restricted access to the rest of your device/network).

5. **Keep your devices and software up to date**: Ensure staff click on any updates to software/applications issued by the manufacturers/developers, as these fix security vulnerabilities in addition to adding new features.

Firms should, as a matter of good practice, review the guidelines on the Cyber Essentials website and complete the checklists on the 'advice' page (you are advised to keep a record of your completed checklist):

https://www.cyberessentials.ncsc.gov.uk/advice/

9.1. Physical Security – Factors to consider

The ICO's guidance on security suggests that Firms look at the following factors when reviewing the Firm's physical security:

Access (pre-entry)	Review the quality of doors and locks and the protection of the premises by alarms, security lighting or CCTV.
Access (post-entry)	How is physical access controlled, e.g. visitor passes, on-duty receptionist/onsite security officer, temporary fob access to restricted areas
Disposal of data	Check how hard copies of personal data are destroyed, e.g. office shredder, secure disposal outsourced to third party (what due diligence performed at outset)? Electronic waste, e.g. decommissioning of computers/devices.
Storage	How is IT equipment stored, and how secure are mobile devices? Are cabinets containing hard copies of personal data lockable/fob-entry room?

10. Requirements on Data Processors?

If one or more organisations process personal data on our behalf, these are data processors under GDPR. As data controller, we remain responsible for ensuring compliance with GDPR. However, the data processor must also comply with the security provisions under GDPR.

Data controllers using a data processor must ensure that they obtain the following assurances from a Data processor which is processing data on their behalf:

- Obtain sufficient guarantees from the data processor about its security measures;
- Ensure that the contract stipulates that the processor takes all measures appropriate to the nature, scope, context and purposes of processing under Art 32 of GDPR ('security of processing'), i.e.
    - Pseudonymisation and encryption of personal data
    - Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
    - Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident
    - Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures ensuring the security of the processing.
- Ensure that the contract includes a requirement that the processor makes available all information necessary to demonstrate compliance, i.e. to enable the Firm/authorised third party to audit and inspect the processor

11. Staff Training

Any person acting under the Firm's authority and with access to personal data must process that data only where they have been explicitly instructed to do so. The ICO also interprets this provision as requiring Firms to train staff so that they understand the Firm's security policy and procedures relating to personal data.

We will conduct both initial and refresher training, which will include the following topics:

- The Firm's responsibilities as a data controller
- Staff responsibilities for protecting personal data – outlining that they may commit a criminal offence if they deliberately access or disclose personal data without authority.
- Proper procedures to identify callers
- The Dangers of people attempting to get hold of personal data by deception (incl. how to identify 'phishing' attacks or encouraging staff to alter information when they are not permitted to do so).
- Restrictions on the personal use of systems by staff e.g. to avoid computer viruses/spam).

We will include a high-level summary of GDPR as part of our annual regulatory and financial crime training provided to all staff and notify staff where the Firm's GDPR policies are located.

12. Record keeping

The Compliance Officer is responsible for the Firm's data retention procedures and should ensure that all records are maintained as required under Article 30 of GDPR. The Firm will ensure that its accountability framework remains aligned with evolving UK data protection requirements, including any changes introduced under the Data (Use and Access) Act 2025.

We will maintain such records using the ICO pro forma templates that can be found here, and include a template for both Controllers and Data Processors:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

12.1. Data Retention periods

In establishing the Firm's data retention periods, we must:

- Consider applicable legal, compliance and data protection requirements;
- Consult with senior management and staff on the collection, storage and archiving of data;
- Identify both internal and external entities that collect, store or archive Firm data; and
- Consider specific retention requirements for sensitive data and procedures for handling stored information during litigation periods.

During the data retention period, the Compliance Officer is responsible for ensuring that archived data is retrievable. This includes ensuring that, as and when new software or hardware is implemented, the IT team verifies that the new system(s) can read legacy data and that encrypted data is easily retrievable.

When establishing retention periods, the Compliance Officer may seek to rely on the Information Commissioner's Office (ICO) guidance:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/