The BSS Group Pension Scheme

DATA PROTECTION POLICY

JUNE 2025

GOWLING WLG

CONTENTS

THE BSS GROUP PENSION SCHEME

DATA PROTECTION POLICY

VERSION 2.0

1 TERMS AND ADOPTION

1.1 **SCOPE:**

(a) This policy sets out the principles and responsibilities for protecting data relating to the BSS Group Pension Scheme (the "**Scheme**") (the "**Policy**"). Key terms and phrases relating to data protection are explained in more detail in the glossary (see page 13 of the Policy).

(b) This Policy has been commissioned, considered and adopted by Ross Trustees Services Limited, (the "**Trustee**"). The Policy was last revised in June 2025.

2 PRINCIPLES AND RESPONSIBILITIES

2.1 **INTRODUCTION:**

(a) **About the Policy**

The processing of personal data in the UK must be compliant with the Data Protection Act 2018 ("**DPA**"), as well as other related legislation which is applicable including complying with the General Data Protection Regulation ("**UK GDPR**") and the **Data Protection Laws**.

(b) **Why is this Policy relevant?**

(i) The Policy forms part of the Trustee's approach to complying with the Data Protection Laws and records how the Trustee will apply data protection principles in practice.

(ii) The Policy will help the Trustee to manage risks involving a breach relating to the Scheme Personal Data. A breach of the Data Protection Laws can result in the Information Commissioner's Office ("**ICO**") imposing significant fines on controllers and processors. Breach of the Data Protection Laws can have very serious financial, regulatory and reputational consequences and can even be a criminal offence.

(iii) The maximum penalty that may be imposed by the ICO may be up to £17.5 million, or 4% of the total annual worldwide turnover, whichever monetary value is higher. For schemes, 'worldwide turnover' would likely be interpreted as total scheme assets.

(c) **When does the Policy apply?**

(i) This Policy applies whenever the Trustee processes personal data relating to members, other beneficiaries or potential beneficiaries of the Scheme (the "**Scheme Personal Data**") but also personal data of any suppliers, of the sponsoring employers or any other individuals with whom the Trustee has interactions.

(ii) Key terms and phrases relating to data protection are explained in more detail in the glossary (see page 13 of the Policy), but here are the most important ones:

(A) **Personal Data** means any information relating to a living, natural person who is identified or identifiable from the data. Someone is identifiable if they can be identified by a specific piece of data (e.g. National Insurance number or full name) or a combination of data (e.g. date of birth and postcode).

(B) **Processing** means almost any use of personal data. This is a wide definition and includes almost anything you can do with personal data (such as collecting, recording, organisation, structuring, amending, retrieval, consulting, using, disclosure, storing (whether you access it or not) and deleting). This applies regardless of whether the data is held on paper or in an electronic format (e.g. on computers, laptops, online storage, email, memory sticks etc.).

(iii) The Trustee will usually be considered a controller under the Data Protection Laws in respect of the Scheme Personal Data and for other personal data it processes in the course of carrying out its responsibilities. This means that the Trustee is responsible for complying with the Data Protection Laws when processing the Personal Data. This applies regardless of whether that data is held on paper or in an electronic format (e.g. on computers, laptops, online storage, email, memory sticks etc.).

(d) **When does the Trustee process Scheme Personal Data?**

(i) There are many possible activities which it may be involved with which involve the processing of the Scheme Personal Data. These might include:

(A) filing, storing and using member data records for general purposes of administering the Scheme;

(B) obtaining quotations from insurance companies and other third parties;

(C) seeking advice or requesting services from professional advisers;

(D) responding to requests from the employers;

(E) responding to requests from scheme members, their families or other third parties connected to them;

(F) implementing Court Orders and Pensions Ombudsman determinations and dealing with tax and other regulatory authorities; and

(G) specific liability management projects (e.g. enhanced transfer value exercises, longevity swaps etc.).

(ii) The Trustee may process other personal data in its day to day interactions with employees of the sponsoring employer, appointing suppliers and handling matters with its professional advisors.

(e) **What is the Trustee's approach to applying data protection principles in practice?**

(i) The Trustee notes that although much of the data processing in relation to the Scheme is outsourced to third parties, the Trustee is ultimately responsible for compliance with the Data Protection Laws in its role as a controller.

(ii) The Trustee also notes that the Data Protection Laws embrace a risk-based approach to data protection and that the ICO has issued guidance stating that controllers are expected to put into place comprehensive but proportionate governance measures.

(iii) The Trustee will therefore incorporate data protection into its overall approach to risk management and will focus on higher risk areas in order of priority.

3 THE DATA PROTECTION PRINCIPLES

Both the DPA and the UK GDPR contain six thematic principles and an additional overriding principle that all controllers must comply with when processing personal data.

3.1 Overview of the Data Protection Principles

Lawful, fair and transparent - personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals.	**Accuracy -** personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay (having regard to the purposes for which it is processed).
Purpose limitation – personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	**Storage limitation -** personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
Data minimisation - personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed.	**Integrity and confidentiality -** personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction of or damage to that data, using appropriate technical or organisational measures.
Overriding principle – Accountability Controllers are: (a) responsible for; and (b) required to be able to demonstrate compliance with the data protection principles outlined above.	

3.2 How will the Trustee Apply the Data Protection Principles in Practice?

This Policy has been drafted in line with the data protection principles. The following sections describe how the Trustee will apply each of the data protection principles in practice when processing the Scheme Personal Data.

4 PRINCIPLE ONE - PROCESSING PERSONAL DATA FAIRLY, TRANSPARENTLY AND LAWFULLY

4.1 Fair and Transparent Processing

(a) To process personal data fairly and transparently, the Trustee needs to make sure that it only processes the Scheme Personal Data if the individual to whom it relates has been given certain information, including:

(i) who the controller is (in this case the Trustee);

(ii) the purposes for which the data is to be processed by the Trustee and the lawful grounds for processing;

(iii) in what circumstances, and to what types of organisations data may be disclosed or transferred; and

(iv) how long data will be kept and how it will be secured.

(b) This will be set out in privacy notices which the Trustee makes available to Scheme members, beneficiaries and other individuals whose personal data the Trustee processes. The privacy notice for Scheme members and beneficiaries is available on the Scheme's website.

(c) An exception to this general rule applies in respect of individuals named in a member's expression of wish form. The Trustee will keep such nominations confidential, even from the people nominated in them as communicated to members. As a result, it would go against the Trustee's other legal duties if it issued a privacy notice to such nominated individuals. The Trustee will provide such individuals with the Scheme's privacy notice if they ultimately become a beneficiary of the Scheme or become aware that they are being considered for benefits under the Scheme.

4.2 Lawful Grounds for Processing

In order to process data lawfully, the Trustee must satisfy one or more of the lawful grounds for doing so for each processing activity that it undertakes. These lawful grounds are set out in the Data Protection Laws. The lawful grounds that are most relevant to the Trustee are summarised in Table A (for all personal data) and **in addition** to those, where the Trustee processes Special Categories of Personal Data (see the Glossary for the definition of this term), the Trustee must also satisfy one of the grounds set out in Table B.

(a) TABLE A: Lawful Grounds for Processing Personal Data

The Trustee will take reasonable steps to ensure that any personal data is processed only if at least one of the lawful grounds set out below applies:

Legal obligations	Processing is carried out to comply with a legal obligation placed on the Trustee (including both specific pensions legislation and common law obligations such as the Trustee's fiduciary duties). The Trustee is subject to legal obligations set out in legislation and common law (notably, trust law). Many of these legal obligations require the Trustee to process certain personal data. Such obligations include (but are not limited to) those found in trust law (i.e. the Trustee's fiduciary duties) and in statute (e.g. as set out under certain parts of the Pension Schemes Act 1993, the Pensions Act 1995, the Pensions Act 2004, and the Finance Act 2004 (and various other subsequent Finance Acts), and under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. This ground does not apply to any contractual obligations but it could apply to any data which was required by The Pensions Regulator under its statutory powers.

	It is essential for the Trustee to process the Schemes' Data in order for it to comply with its legal obligations.
Legitimate interests	Processing is carried out to pursue the Trustee's legitimate interests (e.g. collecting personal data from Scheme members in order to pay Scheme benefits) or the legitimate interests of a third party (e.g. if information is shared with the Scheme's employer for the purpose of helping the employer comply with their regulatory requirements). This condition only applies if the processing does not adversely affect the interests or fundamental rights and freedoms of the individual concerned. If there is a serious mismatch of competing interests between the Trustee and the individual, the individual's interests will have priority over business interests. The Trustee will carry out a legitimate interests balancing test as appropriate, for example where the Trustee's processing falls outside of the Trustee's 'core' / BAU activities.
Public task	Processing is necessary for the performance of a public task.
Consent	The individual has provided consent. In order to be valid, the individual's consent must be satisfy certain strict criteria. For more information on what constitutes valid consent, please see the heading ' What constitutes valid and explicit consent?' below. Generally speaking, the Trustee will not rely on the consent of the data subjects as its lawful ground for processing personal data.
Contract	Processing is carried out to enter into a contract between the Trustee and the individual or to perform such contract. As the Scheme is a trust-based arrangement, this ground will not normally provide a legal ground for processing personal data relating to members of the Scheme.

(b) **TABLE B: Exemptions Permitting the Processing of Special Categories of Personal Data**

Employment and social security obligations	Processing is necessary for the purposes of carrying out the Trustee's obligations in connection with employment, social security or social protection law (which are European-based references to pensions), or a collective agreement such as sick pay administration. The Trustee has an Appropriate Policy Document in place, as required by the Data Protection Laws, for processing Special Categories of Personal Data under this ground.
Publicly available information	Processing is carried out where it relates to the personal data manifestly made public by the data subject. This will only be used exceptionally by the Trustee.

Substantial public interest	Processing is necessary for reasons of substantial public interest. This will only be used exceptionally by the Trustee, and the Trustee will identify the relevant part of the DPA.
Legal rights	Processing is necessary for the establishment, exercise or defence of legal claims. The Trustee will use this if necessary to exercise its legal rights or to defend itself from claims.
Explicit consent	Processing is carried out with the explicit consent of the data subject. For all of its core activities, the Trustee will not rely on the explicit consent of the data subjects as the Trustee *needs* to process personal data to comply with its legal obligations and could not comply with those obligations without processing personal data.

4.3 **When Might Consent or Explicit Consent be Used?**

(a) In exceptional circumstances only, where the data subject has a genuine choice about the Trustee's processing of their data, the Trustee may seek the member's consent for the processing of personal data or explicit consent for the processing of Special Categories of Personal Data. Generally, the Trustee will not rely upon consent. This is because:

(i) individuals can withdraw consent at any time. In such cases, the Trustee may have to stop processing this data. This will take time to sort out and could complicate systems; and

(ii) ICO guidance says that organisations should not rely on consent where any other condition is available.

5 PRINCIPLE TWO - PURPOSE LIMITATION

5.1 The Trustee will take appropriate steps to ensure that the Scheme Personal Data is only processed if that processing is compliant under the original purpose for which this data was originally collected. Before processing a member's personal data for another purpose the Trustee will:

(a) ensure that the new purpose for the processing is compatible with the original purpose (e.g. scientific or historical research purposes, or statistical purposes);

(b) ensure that one of the legal grounds set out above is met; and

(c) notify the data subject of the new processing of their personal data.

5.2 The Trustee will apply the principle of purpose limitation by ensuring that the legal ground for processing is considered before beginning work on any new project or process that will use the Scheme Personal Data.

6 PRINCIPLE THREE - DATA MINIMISATION

The Trustee only collects personal data that is relevant to the Trustee's legal duties and ensures that all data requested is adequate for, and limited to, those purposes. The Trustee will not collect any personal data which is not necessary for its stated purposes. The Trustee will work with its third party service providers to achieve data minimisation where appropriate and without compromising the Trustee's legal duties.

7 PRINCIPLE FOUR - ACCURACY

7.1 Personal data must be accurate and, where necessary, kept up to date.

7.2 The Trustee will take appropriate steps to ensure the accuracy of personal data held on its systems by:

(a) receiving reports from time to time from the Scheme's administrators on the quality and accuracy of the personal data held by the Trustee;

(b) carrying out periodic data audits to check the accuracy of personal data held on its (or its third party service providers) systems;

(c) including a request for members and beneficiaries to update its details in communications issued by the Trustee from time to time; and

(d) requiring its third party administrators to amend or destroy inaccurate data promptly and to ensure that its systems have a single point of truth in respect of each identifiable beneficiary.

8 PRINCIPLE FIVE - STORAGE LIMITATION

8.1 Personal data should not be kept longer than is necessary for the purpose for which it was obtained. This means that personal data should be destroyed or erased from systems when it is no longer required.

8.2 Given the long term nature of managing a pension scheme and the nature of the data held by the Trustee relating to members, their dependants and beneficiaries and to the possibility of claims being brought against the Trustee (which the Trustee ought reasonably be in a position to defend), the Trustee considers that it is generally necessary to keep such Scheme Personal Data for the lifetime of the Scheme plus 15 years.

8.3 The Trustee will review the Scheme's retention period above on a periodic basis and if there is a relevant material change affecting the Scheme. It will also consider from time to time whether there are any exceptions to the general retention approach outlined above.

9 PRINCIPLE SIX - INTEGRITY AND CONFIDENTIALITY

9.1 Any disclosure of personal data must be subject to appropriate security safeguards and, depending on the nature of the personal data, confidentiality obligations.

9.2 The Trustee will ensure that any sharing of the Scheme Personal Data will be subject to appropriate security safeguards, including as appropriate:

(a) where any of the Scheme Personal Data is kept in order to maintain accurate records but is no longer needed for the day to day running of the Scheme, the Trustee will consider the secure archiving of paper records and moving electronic files to secure offline storage;

(b) where personal data is no longer to be retained, the Trustee will comply with a safe disposal process for the destruction of hard copy and electronic files containing personal data;

(c) where appropriate, the Trustee will consider anonymisation and Pseudonymising any of the Scheme Personal Data that is included in meeting packs, advice and emails by using scheme specific or case specific reference numbers rather than identifying details such as the member's full name, date of birth etc.;

(d) the Trustee will ensure that any sharing of Scheme Personal Data will be subject to appropriate security safeguards, such as email distribution controls so that emails that include or attach the Scheme Personal Data are only shared with those who need to have access to the information. The Trustee will

require its third party service providers to take care when sending or replying to email messages with recipients in different organisations and will keep that under review;

(e) the Trustee will restrict access to documents that include Scheme Personal Data to those who need to have access. This may include (where appropriate):

(i) password protection;

(ii) implementing access controls at a system level so that only specific individuals can access Scheme Personal Data; and

(iii) applying similar controls to the physical access to hard copy documents.

9.3 As most of the day to day processing of the Scheme Personal Data is carried out by third parties, the Trustee will also ensure that its contracts with those third parties contain clauses requiring the service provider to implement appropriate safeguards of technical and organisational security to protect against unauthorised or unlawful processing and against accidental loss, destruction of or damage to, personal data.

9.4 The Trustee will also liaise with the Scheme's key third party service providers to get sufficient comfort that:

(a) they have and will put in place appropriate data security measures;

(b) they have put and will keep in place appropriate technical and organisational measures that will ensure the ongoing confidentiality, integrity, availability and resilience of systems and services than involve the processing of the Scheme Personal Data;

(c) they have the ability to restore the availability and access to the Scheme Personal Data in a timely manner in the event of a physical or technical incident; and

(d) they have implemented a process for testing, assessing and evaluating the effectiveness of the Trustee's and third parties' technical and organisational measures for ensuring the security of the processing.

10 OVERRIDING PRINCIPLE - ACCOUNTABILITY

10.1 Under the overarching principle of accountability, the Trustee, as a controller in respect of the Scheme Personal Data, is:

(a) responsible for complying with the data protection principles; and

(b) required to be able to demonstrate it has complied with the data protection principles.

10.2 The Trustee will apply the principle of accountability by:

(a) maintaining a data protection policy which states how the Trustee complies with data protection principles;

(b) with regard to Special Categories of Personal Data, where required, maintaining an Appropriate Policy Document;

(c) ensuring that each trustee receives training on data protection;

(d) ensuring that any decisions required to achieve compliance are made by appropriately trained and informed individuals and that records are kept of those decisions;

(e) retaining information relating to its audit of how its third party service providers give sufficient guarantees that they have implemented appropriate technical and organisational measures to ensure compliance with the UK GDPR and ensure the rights and freedoms of individuals;

(f) adding non-compliance with the Data Protection Laws to the risks faced by the Scheme in its risk register; and

(g) putting in place a periodic assessment of compliance with the Data Protection Laws and reporting on this at a trustee meeting.

11 OTHER AREAS OF COMPLIANCE

11.1 **Working with Third Parties**

(a) Before the Trustee shares the Scheme Personal Data with third parties, it will:

(i) ensure that the Trustee has a lawful ground for sharing the Scheme Personal Data;

(ii) ensure that the transfer will be in line with the data protection principles;

(iii) ensure it is comfortable that the third party:

(iv) understands its obligations and responsibilities when processing the Scheme Personal Data; and

(v) is capable of meeting the legal requirements of the UK GDPR and, in particular, that it can carry out the processing in line with the data protection principles;

(vi) include a minimum set of clauses in the contract with the third party, including obligations around security and reporting breaches. If the third party is a processor on behalf of the Trustee, as a controller, the Trustee will ensure that this contract includes the required clauses set out Article 28 of the UK GDPR to the reasonable satisfaction of the Trustee as far as possible in the context of commercially negotiated contracts with arm's length third parties;

(vii) consider whether information will be transferred outside of the United Kingdom and if so, ensure that the third party has committed to transfer in accordance with the Data Protection Laws; and

(viii) ensure that the transfer and the processing to be carried out by the third party is covered by the Scheme's privacy notice.

(b) In addition, during the life of any agreement with the third party, the Trustee may decide to carry out periodic assessments, audits or inspections and/or obtain written statements or copies of reports from the third party to check the third party's compliance with the Data Protection Laws. The Trustee will take a risk-based, proportionate approach to this.

11.2 **Data Subject Rights Requests**

(a) Data subjects are granted various rights by the Data Protection Laws. They can request that the Trustee do various things with their personal data and the Trustee has to respond within specified time limits. The Trustee will deal with data subject rights requests in line with its data subject rights request framework. However, given the Trustee's legal obligations, it may be that in some circumstances, those obligations must take precedence over certain data subject rights.

(b) The Trustee will deal with data subject rights requests in accordance with Annex 1.

11.3 **Data Protection Impact Assessments**

(a) Data protection impact assessments are a way of ensuring that processes and systems are privacy-friendly and comply with the Data Protection Laws. They can be used as a tool to assess and manage risks to privacy and document the decisions taken by the Trustee.

(b) If the Trustee becomes involved in a material project which is deploying new technology or a new process which involves processing of the Scheme Personal Data which could impact the rights and freedoms of individuals or which otherwise contains the factors identified by the ICO as requiring a data protection impact assessment, the Trustee will carry out a data protection impact assessment.

11.4 **Reporting breaches of the Data Protection Laws**

(a) The Trustee must report certain breaches of the Data Protection Laws to:

(i) the ICO without undue delay and where feasible, within 72 hours of becoming aware of the breach and, where a notification is not made within 72 hours the Trustee shall include, with the report, reasons for the delay; and

(ii) affected individuals, without undue delay, where the breach is likely to result in a **high risk** of adversely affecting their rights and freedoms.

11.5 The Trustee will seek to include in its contracts with third parties an obligation on the third party to report any breach of the Data Protection Laws relating to the Scheme Personal Data without undue delay. The Trustee will deal with data breaches in line with its breach reporting framework set out in Annex 2.

11.6 **Changes to this Data Protection Policy**

The Trustee reserves the right to change this Policy at any time without notice. The Trustee last revised this Privacy Standard on December 2024.

12 KEY TERMS AND PHRASES USED IN THIS POLICY

Controller	means the natural or legal person or other body who, alone or jointly with others, determines the purposes and means of the processing of personal data. This means that the controller exercises overall control over the 'why' and 'how' of a data processing activity.
Data Protection Act 2018 (DPA)	is the principal legislation that currently applies to the processing of personal data.
Data Protection Laws	means the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and the General Data Protection Regulation as implemented in the UK, together with regulatory guidance and codes of practice issued by the Information Commissioner's Office.
Data protection principles	means the principles that are set out in the Data Protection Laws relating to the processing of personal data. In the General Data Protection Regulation, there are six principles: • lawfulness, fairness and transparency; • purpose limitation; • data minimisation; • accuracy; • storage limitation; and • integrity and confidentiality. In addition, there is an overarching principle of accountability.
Processor	means a natural or legal person or other body who processes personal data on behalf of the controller.
Data subject	means the identified or identifiable living individual to whom personal data relates.
General Data Protection Regulation (UK GDPR)	is the primary EU legislation that, on and from 25 May 2018, applies to the processing of personal data in all member states of the EU. The UK GDPR is retained in UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018.
Information Commissioner's Office (ICO)	is the UK's national data protection authority. It is a public body that is charged with regulating information rights, public sector transparency and individual's privacy in the UK.

Personal data or Personal information	means any information relating to an identified or identifiable natural person; 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 etc.
Privacy notice	means the information that is provided to inform individuals about what you do with personal data. Under the Data Protection Laws, controllers must provide accessible information to individuals about the use of their personal data.
Processing	means 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.
Pseudonymising	is a data security measure whereby specific, identifying information is removed from a set of personal data so that an individual can no longer be identified without the use of additional information. For example, names and addresses might be removed from a set of member data, with individual records identified by a unique identifier (e.g. a scheme number). If the additional information is kept securely and separately, pseudonymisation will mitigate the risk that a data protection breach will adversely affect individuals.

Special categories of personal data	means:
	• personal data that is personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
	• 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.

Technical and organisational measures	means the steps that are taken by a controller in order to ensure, and to be able to demonstrate, that processing is performed in accordance with the UK GDPR. The UK GDPR does not specify which measures are required, but it does highlight Pseudonymisation as a method of increasing the security of personal data.

ANNEX 1

DATA SUBJECT RIGHTS REQUESTS

1 Data Subjects' Rights Under UK GDPR

1.1 Under the UK GDPR, individuals (known as "data subjects") have various rights in respect of the processing of personal data that relates to them.

1.2 Paragraphs 1.3(a) to 1.9(a) below set out the individual rights that are available for data subjects to request under the GDPR.

1.3 **The Right to Request Access**

(a) Data subjects have the right to access their personal data and supplementary information processed by a controller. This right, exercised through a Data Subject Access Request (**DSAR**), helps individuals understand and verify the processing of their data in compliance with UK GDPR. It is the most frequently used right under the current data protection regime (see section 3 for further detail).

1.4 **The Right to Request Rectification of Personal Data that is Inaccurate or Incomplete**

(a) Data subjects have the right to request the rectification of any inaccurate or incomplete personal data concerning them.

(b) If a Trustee shares inaccurate personal data with a third party, it should notify the third party of any corrections if the data is still in use. For significant amendments, the Trustee should also document the changes and the context in which they were made.

(c) The Trustee must notify the data subject that the incorrect data has been rectified or the incomplete data has been completed. This response must be in the format and within the time limits set out in section 5 below.

1.5 **The Right to Request Erasure (or the 'Right to be Forgotten')**

(a) Data subjects have a right to request to have their personal data erased so it can no longer be used where:

(i) the data subject believes that the Trustee no longer needs to process it for the purposes for which it was collected or originally processed;

(ii) consent was withdrawn and no other legal basis exists;

(iii) the data subject has objected to the Trustee's processing; or

(iv) the personal data was processed unlawfully or should have been erased.

(b) If the Trustee shared this data with other controllers, it must inform them of the erasure request.

(c) The Trustee should confirm that the data has been erased, or otherwise provide reasons why the data will not be erased– though there are exemptions to this rule (see section 3.5(e)(iv)). This response must be in the format and within the time limits set out in section 5.

1.6 **The Right to Request Restriction of Processing**

(a) The right to restrict processing gives individuals the right to restrict the processing of their personal data in certain circumstances. This allows the data subject to limit the way in which the Trustee processes and uses their personal data. This right requires the Trustee to suspend processing where:

(i) the data subject disputes the accuracy of their data;

(ii) the processing is unlawful, but the data subject does not want their data erased;

(iii) the Trustee no longer needs the personal data for the purposes of its processing, but the data subject requires the data in order to establish, exercise or defend his/her own legal claim(s); or

(iv) the data subject has objected to processing (see paragraph 1.8 below).

(b) If the Trustee's processing is restricted in any of the circumstances described above, whilst the restriction is active it must notify the data subject before lifting it. The Trustee must also communicate any restriction to third parties processing personal data unless it is impossible to do so or requires a disproportionate effort.

(c) The Trustee can store the personal data during the restriction but cannot do anything else with it.

(d) The Trustee must confirm for the data subject that processing of the data has been restricted or provide reasons why it will not restrict processing of data. This response must be in the format and within the time limits set out in section 5.

1.7 **The Right to Data Portability**

(a) This right only applies where the lawful ground of processing is performance of a contract. Therefore, this will not apply for the Scheme Personal Data.

(b) The data subject has the right to request the Trustee to provide their personal data in a structured machine-readable, easily transferable format that the individual can move to another organisation or to allow them to use it themselves. Where necessary, the data subject has the right to request the Trustee to transmit this data directly to another controller.

1.8 **The Right to Object to Processing**

(a) Where the Trustee is processing based on its legitimate interests or for direct marketing, data subjects can object to this processing. The Trustee can only continue to process if its legitimate interests override the rights and freedoms of the data subject or to exercise or defend legal claims. The Trustee should confirm the position with its legal advisers if it is in any doubt as to the balance between legitimate interests and data subjects' rights and freedoms.

(b) The Trustee must confirm that the data will no longer be processed or alternatively provide details of why the request will not be fulfilled (i.e. compelling grounds for processing which override the interests, rights and freedoms of the data subject or defence of legal claims) in the format and within the time limits set out in section 5.

1.9 **The Right not to be Subject to a Decision when it is Based on Automated Processing or Profiling which Produces a Significant Legal Effect or Similar on the Data Subject**

(a) Data subjects have a right not to be subject to an automated decision, without any human involvement, which has a legal or similarly significant effect on them. This is highly unlikely to be relevant for Scheme Personal Data.

2 IS A DATA SUBJECT'S REQUEST VALID?

2.1 The Trustee should consider two factors to determine if a valid request has been made:

(a) is the right available in respect of the processing?

(b) have the formal requirements been met?

2.2 Is the Right Available in Respect of the Processing?

(a) Processing is only lawful if one of the six lawful grounds set out in the UK GDPR applies. As set out in the table below, there are certain rights which are not available when some of the lawful grounds apply to the processing of personal data.

Data subject right	Lawful ground for processing personal data				
	Consent	Contract	Legal obligation	Public task	Legitimate interests
Access	✓	✓	✓	✓	✓
Rectification	✓	✓	✓	✓	✓
Erasure	✓	✓	×	×	✓
Restriction of processing	✓	✓	✓	✓	✓
Portability	✓	✓	×	×	×
Objection	✓	×	×	✓	✓*
Automated decision making	✓	×	✓	✓	✓

* the Trustee must stop processing following an objection request unless the Trustee can show that its legitimate interests are compelling enough to override the individual's rights.

2.3 Have the Formal Requirements Been Met?

(a) For any of the data subject's requests outlined in section one to be valid, they must comply with the following requirements:

(i) **Has a request been made?**

(A) A request can be made either orally (e.g. over the telephone or in person) or in writing (e.g. by letter or email).

(B) There is no specific format that data subjects have to use for a request to be valid. If there is any doubt as to whether an individual is seeking to make a request, the Trustee should seek confirmation from the data subject.

(ii) **Has the request been made to the Trustee?**

(A) The request should not, for example, be submitted to third party processors of the Trustee who are only dealing with the personal data in their capacity as processors.

(B) The Trustee should always ensure that any processors it is using are contractually obliged to assist the Trustee with any data subject access requests.

(iii) **Has the request been submitted by the data subject themselves?**

(iv) The general requirement is that a request should be made by the data subject themselves, unless a third party has been properly authorised by the data subject to make the request on their behalf (e.g. a lawyer, legal representative, or someone with a power of attorney). The Trustee will take steps to verify that the person making the request is the data subject, or if a third party makes a request on behalf of a data subject, the Trustee will ask to see a copy of the written appointment.

(A) There are some exceptions to this general requirement**:**

1) where an individual does not have mental capacity to handle their own affairs or where the request relates to a minor. Although such exceptions are unlikely to be relevant, they may still apply.

2) the data subject provides reasonable ID (ie. a copy of their passport or driving licence). The controller must be careful not to disclose data to someone who is not the data subject (or authorised on the data subject's behalf).

3) the Trustee may waive the requirement for ID in circumstances where the data subject's identity is not in doubt (e.g. where the request is made in person or in the course of litigation).

(B) If there is no evidence that a third party is authorised to act on behalf of a data subject, the Trustee is not required to respond to the DSAR. However, if the Trustee is in possession of the data subject's contact details, the Trustee may respond to the data subject directly to confirm whether or not the data subject wishes to make a DSAR.

(v) **Is the request sufficiently clear to enable the Trustee to comply with it?**

(A) If the request is not sufficiently clear, the Trustee should request clarification from the data subject as soon as possible.

(B) For data subject access requests in particular, it is helpful if the data subject can be specific in their request so that the Trustee is more likely to locate the data they require (e.g. data processed between certain dates, in certain systems, by particular teams or for particular reasons). However, the Trustee cannot require data subjects to narrow their requests.

3 DATA SUBJECT ACCESS REQUESTS

3.1 The most frequently used data subject right is the Data Subject Access Right ("**DSARs**") which enables data subjects to request a wide variety of information trustees may hold in relation to them.

3.2 Under the GDPR, charges cannot be made for a DSAR unless the request is excessive or unfounded (see sections 4.2(a) and 4.2(b)), or if an individual requests multiple copies of their data. In this instance the fee will be based on the administrative cost of providing the information.

3.3 The Trustee shall notify the data subject promptly to inform them should they decide to charge a fee for the request. The Trustee does not need to comply with a request until this fee has been paid.

3.4 **What does the Controller have to tell Individuals?**

(a) The data subject access right entitles individuals to ask for:

(i) a copy of their personal data (see 3.5 below for information on how to find this);

(ii) details of the purpose for which it is being, or is to be, processed;

(iii) the categories of personal data concerned;

(iv) details of the recipients or classes of recipients to whom it is disclosed (or might be disclosed);

(v) the period for which it is held (or the criteria used to determine how long it is held);

(vi) the right to lodge a complaint with the ICO;

(vii) the right to request rectification, erasure, and restriction of processing the personal data;

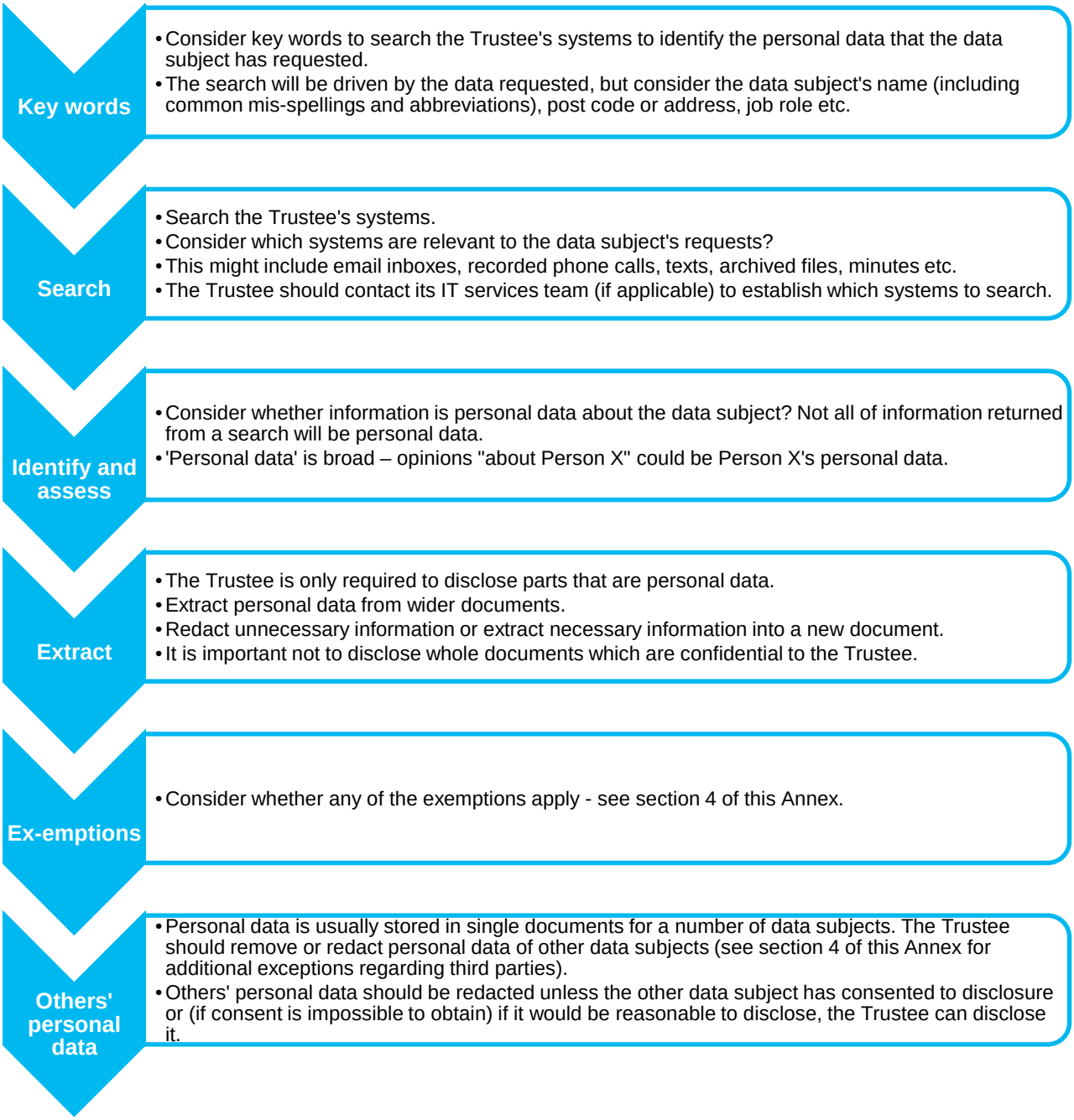
(viii) any details available about where the information has been obtained;

(ix) confirmation as to whether the controller carries out any automated decision-making (including profiling) and, where it does, information about the logic involved and the envisaged outcome or consequences of that decision or profiling; and

(x) details of any transfers to a third country or to an international organisation.

3.5 **What Should be Disclosed?**

(a) Only the data subject's personal data should be disclosed (i.e. not information (i) about other people (ii) which relates to the Trustee or other companies or (iii) within a document in which an individual is named or referred to). The controller should collate the personal data that has been requested in the following way:



(b) When considering whether it would be reasonable to disclose personal data in the last step above, the Trustee should consider:

(i) whether or not the information is confidential;

(ii) how sensitive the information is;

(iii) how likely it is that the other person will suffer damage and/or distress if the information were to be disclosed; and

(iv) if the data subject already knows the identity of the other person. This may require the Trustee to decide whether or not information should be redacted if it isn't possible to obtain consent. This should be considered on a case-by-case basis.

(c) Can the Trustee ask the data subject to be more specific about their request?

(i) If the Trustee processes a large amount of information about a data subject, the Trustee may request the data subject to specify the information or processing activities their request relates to before responding to the DSAR.

(ii) The Trustee should not ask the data subject to narrow the scope of their request. However, the Trustee is permitted to ask for clarifications that will help locate the requested information or if the DSAR is not clear. However, a broad request for "all personal data that the Trustee hold about me" is not considered to be unclear by the ICO. The Trustee can ask a data subject if there is specific information that they are looking for, as this will help it locate it, but data subjects are not required to narrow or limit a DSAR to be more specific about their requests.

(d) What if the Trustee does not hold the personal data that has been requested?

(i) If the Trustee does not hold the personal data that was requested, it should notify the data subject of this as soon as possible (and in any event within 30 calendar days).

(ii) Controllers are entitled to routinely destroy/delete personal data in accordance with their policies and to ensure that they only hold personal data as long as is necessary. However, it is an offence under the DPA for the Trustee to alter, deface, block, erase, destroy (where this is not in accordance with the Trustee's document retention policy), or to conceal personal data requested in a DSAR in order to avoid disclosing this information to the data subject.

(e) Does the Trustee have to disclose the personal data requested?

(i) In the vast majority of cases, yes.

(ii) The Trustee cannot choose not to respond, or to only provide some of the personal data that has been requested because the information shows the employer in an undesirable light. The context in which the request is made is also irrelevant.

(iii) The Trustee cannot refuse to respond because the data subject is using the DSAR in the lead up to potential litigation. If the Trustee fails to respond or withhold data where it is not allowed to that would be a breach of the UK GDPR and could result in an investigation by the ICO and a fine for the Trustee.

(iv) However, there are some exemptions where certain pieces of personal data can be withheld. These exemptions are covered in the next section.

4 EXEMPTIONS AND UNFOUNDED OR EXCESSIVE REQUESTS

4.1 Exemptions

The controller can withhold personal data if it falls into the following categories (but it must inform data subjects that some information processed is subject to an exemption and which exemption(s) apply). In the case of each exemption, the Trustee should be able to demonstrate the rationale behind taking this approach, should the data subject disagree with a response confirming this approach, and therefore makes a complaint ending up with the ICO investigating the matter. The Trustee should not routinely rely on exemptions or apply them in a blanket fashion.

EXEMPTION	COMMENT
Confidential References	Where the controller is an employer, a confidential reference given or received by the controller about an employee or prospective employee is exempt from disclosure.

Legal	Information which is subject to legal professional privilege or litigation privilege is exempt from disclosure.
Crime	Where disclosing information would be likely to prejudice the detection and/or prevention of crime and/or the apprehension and prosecution of offenders, this information will be exempt from disclosure. If disclosure of the information requested could lead to self-incrimination i.e. it could be used as evidence of an offence having been committed by the entity to whom the request is made, the information will also be exempted. This exemption does not apply to an offence under the DP Act 2018, but any information provided to an individual in response to a subject access request is not admissible against the entity to whom the request was made in proceedings for an offence under the DP Act 2018.
Tax	Where disclosing information would be likely to prejudice the assessment or collection of tax or duty or an imposition of a similar nature, the information will be exempt from disclosure.
Management information	Where disclosing information is likely to prejudice management forecasts, planning or other activity in relation to a business, this information will be exempt from disclosure.
Negotiations	Where disclosing information is likely to prejudice negotiations with the data subject, this information will be exempt from disclosure. This might apply, for example, where the information requested relates to a current salary review relating to the data subject or in the event of a legal claim by or against the data subject.
Public records	Where the information requested is available from public records (the exemption only applies if the controller is required to publish the information). For the sake of courtesy, however, the controller should refer individuals to the relevant public records.

4.2 Manifestly unfounded or excessive requests

(a) There is no requirement to comply with Data Subject Access Requests for the same or similar information, where requests are:

(i) manifestly unfounded – The Trustee must be confident that there is an obvious or clear quality to the request being unfounded which should be assessed on a case by case basis; or

(ii) excessive e.g. because they are repeated, with the intention of causing disruption, unless the requests are made at **reasonable intervals**, or it overlaps with other requests.

(b) There are no fixed timeframes for determining what would or would not be a reasonable interval, so this will need to be decided on a case by case basis, considering factors such as the sensitivity of the information, how often records are updated, how difficult the information is to provide and how beneficial the additional information would be over the original request (i.e. is this information likely to change rapidly or unexpectedly?). It is important to note that a request is not necessarily excessive just because the individual requests a large amount of information.

5 HOW AND WHEN SHOULD THE TRUSTEE RESPOND TO A REQUEST?

This section covers the requirements under UK GDPR which apply to all data subject requests in relation to how a response should be given, when it should be given and what to do if the statutory time limit is unachievable or the Trustee is unwilling or unable to comply with a request.

5.1 **How Should the Trustee Respond to a Request?**

(a) The Trustee must respond in writing to the data subject and the response should be "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child".

(b) The UK GDPR does not specify the format in which the information should be provided, as long as it satisfies the requirements in paragraph (a) and is in writing. The following points should, however, be considered:

(i) where possible, data should be provided electronically, especially where the request for data was made electronically;

(ii) anything that is not intelligible, such as handwritten notes or codes, should be made legible (e.g. typed) or deciphered;

(iii) where the data subject is disabled, the controller must consider the most appropriate format for disclosure, such as electronic, braille, audio, etc.; and

(iv) if a data subject wants more than one copy of their data, the controller can charge a reasonable fee based on administrative costs.

(c) No charge can be made for providing the information in accordance with a single valid request.

(d) Controllers should keep a copy of the response that is provided. On an ongoing basis this will clarify:

(i) whether responses to data subject requests are compliant with the requirements under UK GDPR; and

(ii) whether the response was provided within the required time limit. If controllers respond by telephone, they must record the date and time of the response and what was said to the data subject.

5.2 **When Should the Trustee Respond to a Request?**

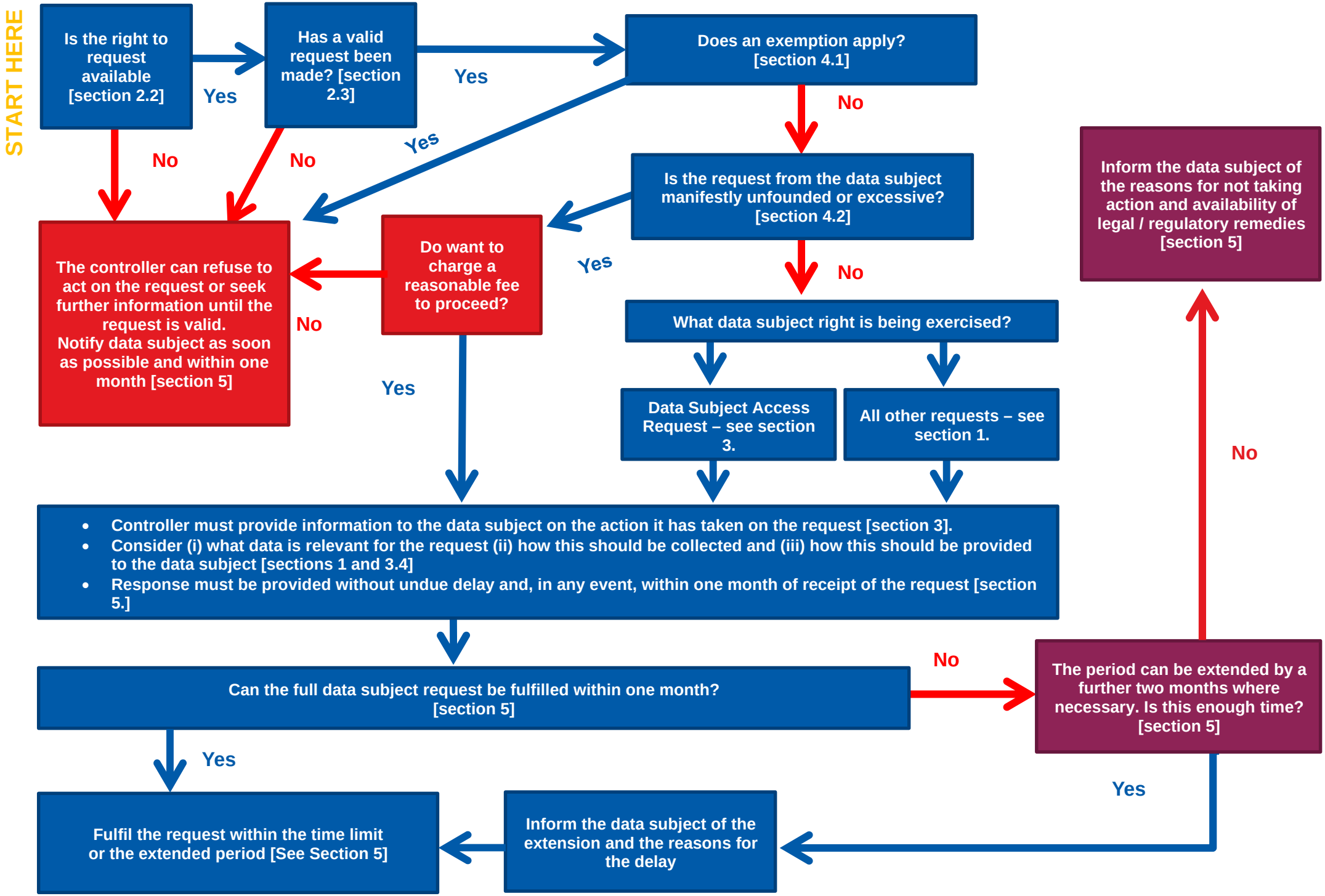
(a) Once a valid request has been received (including a response to any clarification), the time limit starts to run. The Trustee must respond to a data subject rights request without undue delay and in any case **one month**.

(b) If the request is particularly complex, or if the Trustee is trying to respond to a large number of data subject rights requests at once, the time limit can be extended by an additional two months (as long as the Trustee notifies the data subject within thirty calendar days to explain why it requires longer to respond).

(c) If the Trustee is **not going to fulfil the request**, it must inform the data subject without delay and at the latest within one month of receipt of the request. The response should:

(i) provide the reasons for not fulfilling the request; and

(ii) set out the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.


START HERE
Is the right to request available [section 2.2]
Yes
Has a valid request been made? [section 2.3]
Yes
Does an exemption apply? [section 4.1]
No
No
No
Yes
Is the request from the data subject manifestly unfounded or excessive? [section 4.2]
Yes
Do want to charge a reasonable fee to proceed?
No
The controller can refuse to act on the request or seek further information until the request is valid. Notify data subject as soon as possible and within one month [section 5]
No
Yes
What data subject right is being exercised?
Data Subject Access Request – see section 3.
All other requests – see section 1.
Inform the data subject of the reasons for not taking action and availability of legal / regulatory remedies [section 5]
No
Controller must provide information to the data subject on the action it has taken on the request [section 3].
Consider (i) what data is relevant for the request (ii) how this should be collected and (iii) how this should be provided to the data subject [sections 1 and 3.4]
Response must be provided without undue delay and, in any event, within one month of receipt of the request [section 5.]
Can the full data subject request be fulfilled within one month? [section 5]
No
The period can be extended by a further two months where necessary. Is this enough time? [section 5]
Yes
Yes
Fulfil the request within the time limit or the extended period [See Section 5]
Inform the data subject of the extension and the reasons for the delay

ANNEX 2

DATA BREACH REPORTING

1 ASSESSING PERSONAL DATA BREACHES

1.1 What is a personal data breach?

(a) A personal data breach is a **breach of security** leading to the **accidental** or **unlawful**:

(i) destruction of;

(ii) loss or theft of;

(iii) alteration without permission of;

(iv) unauthorised disclosure of; or

(v) access by an unauthorised third party to **personal data** transmitted, stored or otherwise processed.

(b) There are three kinds of breach:

(i) a confidentiality breach;

(ii) an availability breach; and

(iii) an integrity breach.

(c) A breach may be categorised as being in one or more of those categories, for example:

(i) a lost / stolen laptop or tablet containing personal data – this could be categorised as being all three categories of breach, depending on the circumstances;

(ii) sending personal data to an incorrect recipient – this could be categorised as a breach of confidentiality and integrity, depending on the circumstances;

(iii) alteration of personal data without permission – this could result in an availability and integrity breach;

(iv) access by an unauthorised third party – this could be a confidentiality and/or an integrity breach; and

(v) loss of availability of personal data, e.g. encryption by ransomware; loss of decryption key – this would be an availability breach unless the attackers/unauthorised third party could also access the personal data, in which case it could also be a breach of confidentiality and integrity.

1.2 Who is responsible for a personal data breach involving the Scheme's Personal Data?

(a) The Trustee, in its role as controller, is responsible for personal data breaches involving the Scheme's personal data.

In the event of a personal data breach involving the Scheme's personal data, the Trustee will determine the facts in relation to the breach, including the extent of it, and assess the likely risks to the rights and freedoms of any affected individuals. Breaches should be reported to the Nominated Trustee Representatives of RTSL via the scheme email address TPandBSS@weareigg.com.

1.3 How are the Risks to Individuals of a Personal Data Breach Assessed?

(a) A risk to the rights and freedoms of individuals exists when the breach may lead to physical, material or non-material (e.g. emotional) damage for the individuals whose data has been breached, e.g. discrimination, identity theft or fraud, financial loss and damage to reputation.

(b) When the breach involves Special Categories of Personal Data such damage should be considered likely to occur.

(c) Our assessment will take into account:

(i) **Type of breach** – for example, unauthorised disclosure of certain information may have a more significant impact on an individual than if that data were erroneously deleted.

(ii) **Nature, sensitivity, and volume of personal data** – context is relevant and a combination of personal data is typically more sensitive than a single piece.

(iii) **Ease of identification of individuals** – identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details.

(iv) **Severity of consequences for individuals –** where data is improperly disclosed, the recipient is relevant to this assessment. For example, if data has been shared with the wrong person, but that recipient is known and trusted, this will materially lessen the severity of the consequences of the breach. It does not, however, mean that a breach has not occurred. The impact may also be viewed as greater if the effects are longer-term.

(v) **Special characteristics of the individual** – certain categories/characteristics of individuals who may be placed at greater risk of danger as a result of a breach.

(vi) **The number of affected individuals** – the more individuals that are affected, the greater the risk.

ACTION

In the event of a breach, the Trustee will determine the facts in relation to the breach, including the extent of it, and assess the likely risks to the rights and freedoms of any affected individuals.

2 BREACH NOTIFICATION

2.1 Notifying the Information Commissioner's Office (ICO)

(a) Controllers have a legal duty to notify the ICO of certain personal data breaches:

(i) without undue delay; and

(ii) where feasible, within 72 hours

after becoming aware of the personal data breach. Where a notification is not made within 72 hours the Trustee shall include with the report, reasons for the delay.

(b) The duty to notify the ICO applies **unless** the personal data breach is **unlikely** to result in a risk to the rights and freedoms of individuals. There is no penalty for reporting an incident that ultimately turns out not to be a breach, and if in doubt the controller should err on the side of caution and notify. However, at the same time the ICO has expressed concern regarding over-reporting since the introduction of the UK GDPR.

(c) A controller has become “aware” of a personal data breach when they have a reasonable degree of certainty that a breach has occurred that has led to personal data being compromised in one of the three ways set out in the numbered list above.

(d) The emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

(e) A short period of investigation is reasonable during which the controller may not be regarded as being "aware". However, the initial investigation should begin as soon as possible.

When a breach occurs, the Trustee will establish the **likelihood** and **severity** of the resulting risk to people's rights and freedoms in accordance with the above guidelines and notify the ICO where we deem that a risk is likely. The Trustee will notify the ICO once it has established with a reasonable degree of certainty that a breach has occurred and the conditions dictate.

If the Trustee is unable to notify the ICO within 72 hours, the notice will be accompanied by an explanation of the reasons for the delay.

But note that the 72 hours only start to run when the Trustee becomes aware (which may be during the investigation rather than when attention was first drawn to the possibility of a breach).

2.2 **Information to be Provided to the ICO**

(a) The information to be provided to the ICO will include:

(i) a description of the nature of the breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(ii) a description of the likely consequences of the personal data breach;

(iii) one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of personal data or data subjects indicate a risk of particular damage as a result of a breach (e.g. identity theft), it is important to say so;

(iv) the name and contact details from whom more information can be obtained;

(v) a description of the measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects; and

(vi) if applicable, reasons for any delay in making the notification and/or providing information.

(b) If it is not possible to provide all of the information at the same time as the initial notification, the Trustee will notify the ICO first and then provide the rest of the information in phases without undue further delay.

(c) The Trustee will consider whether, owing to the kind of breach (confidentiality, integrity or availability), further information might be needed to fully explain the circumstances.

2.3 **Notifying Affected Individuals**

(a) Controllers have a legal duty to notify affected individuals of any data breaches concerning their personal data if there is a **high risk** to the rights and freedoms of the affected individual. Notification should be sent to the affected individuals without undue delay (which, according to the ICO, means as soon as possible).

(b) Assessing whether there is a **high risk** involves considering both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe and/or the likelihood of the consequences is greater, the risk is higher.

(c) We will likely conclude that we do not need to contact individuals if any of the following conditions are met:

(i) appropriate technical and organisational protection measures (like encryption) were applied to the personal data affected by the breach, so that the personal data is unintelligible to any person who is not authorised to access it;

(ii) the Trustee has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; and

(iii) it would involve disproportionate effort. In those cases, there shall instead be a public communication or similar measure so that the data subjects are informed equally effectively.

The Trustee will inform affected individuals if a breach is likely to result in a **high** risk to the rights and freedoms of individuals. This notice will be given directly to affected individuals and will be sent as soon as possible.

2.4 **Content of Notices to Affected Individuals**

(a) A clear, plain language description of the nature of the breach will be sent to affected individuals in a stand-alone document, which will also contain at least:

(i) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(ii) a description of the likely consequences of the breach; and

(iii) a description of the measures taken, or proposed, to address the breach, including, where appropriate, measures to mitigate its possible adverse effects (e.g. that the controller has received advice on managing the breach and lessening its impact).

(b) The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords if their access credentials have been compromised.

(c) Examples of transparent communication methods include direct messaging, prominent website banners or notification, postal communications and prominent advertisements in print media. The method chosen should maximize the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean employing several methods of communication. The communication may also need to be accessible in appropriate alternative formats and languages.

2.5 **Do we Need to Notify Anyone Else?**

(a) In most instances, the Trustee will be acting as controller in relation to the personal data. If, however, the Trustee is acting as processor (for example, of the Company's data), the breach must be notified immediately to relevant controller in relation to that data (and not to the ICO and/or affected individuals).

(b) In addition, the Trustee will need to consider whether it needs to report a breach of the law to The Pensions Regulator.

(c) The Trustee will assess whether it needs to make notifications to:

(i) other third parties (e.g. police, insurers, professional bodies, bank or credit card companies, to limit the effect on the individuals involved); and/or

(ii) the Pensions Regulator.

2.6 **What Records do we Need to Keep?**

(a) Under the UK GDPR, the Trustee is required to record all breaches, regardless of whether or not they need to be reported to the ICO.

(b) The Trustee will have to document the facts relating to the breach, its effects and the remedial action taken. This is part of the Trustee's overall obligation to comply with the accountability principle.

(c) The Trustee will keep a record of all personal data breaches. This will include:

(i) facts relating to the breach;

(ii) effects of the breach and any remedial action taken;

(iii) where we decide not to notify the breach, our reasons for making that decision.

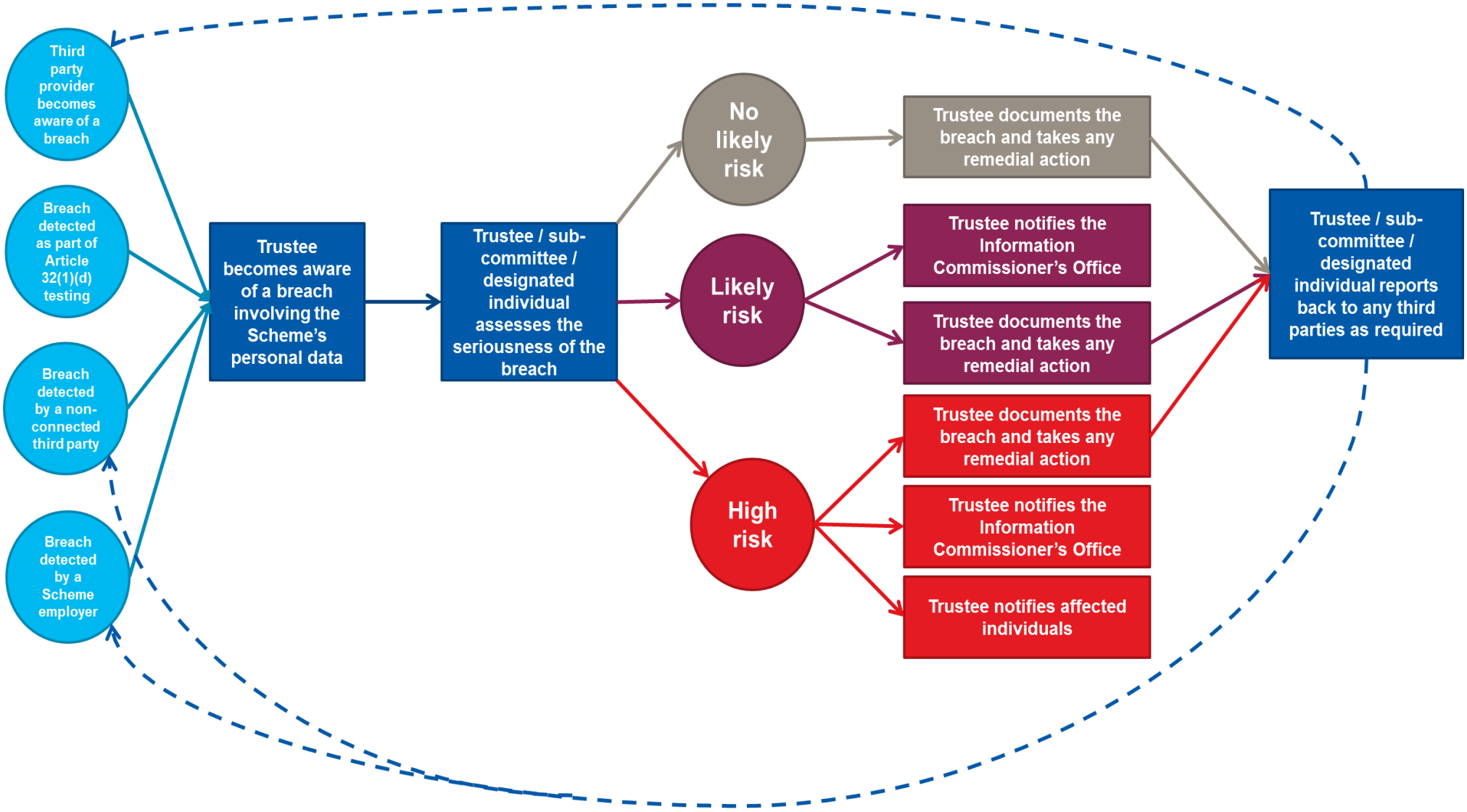
2.7 **What Other Steps do we Need to Consider?**

(a)

(i) The Trustee will immediately act to contain and recover the breach.

(ii) The Trustee will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

Data Breach Step Plan



GOWLING WLG (UK) LLP
T +44 (0)370 903 1000
gowlingwlg.com

GOWLING WLG