



Documented Information and GDPR

Title: Documented Information and GDPR

Contents

1 Documentation Requirements..... 3

2 Business Manual 4

3 Creating and Updating Information 4

4 Control of Documented Information. 4

5 Procedure 7

6 GDPR 12

7 Other References - linked policies and procedures 15

8 Approval, Retention and Issue Details 15

Title: Documented Information and GDPR

1 Documentation Requirements

Documentation has been included within our management system being determined necessary for its effectiveness, being required by legal and other requirements and to meet the necessary criteria for accreditation and continued registration of ***BSEN ISO9001, BSEN ISO 45001, BSEN ISO 14001 and BSEN ISO 27001 to meet customer requirements and applicable 3rd party approvals and schemes.*** Documented evidence is maintained to support compliance to these.

The new General Data Protection Regulations impose stricter control and measures for documented information deemed as personal or sensitive. There is a data protection GDPR policy which defines the obligations and how we meet these obligations. It acknowledges the process of determining which personal and sensitive information we obtain, why we collect it and why we process it, when we do this and the lawful basis for processing. The process appertaining to the rights of individuals in relation to GDPR is included within this section and covers:

- Right to be Informed
- Right to Access
- Right to Rectify
- Right to Restrict Processing
- Right to Object
- Right to Erasure
- Right to Data Portability

The company are not involved with automated decision making and profiling and hence have not covered this in a procedure. Breach under GDPR is detailed in the Control of Non-conforming Process Outputs, Product and Service and GDPR Breach section of the business management system.

Management system documentation includes the QHSE Policy statement. The Policy statement identifies the scope of our business and associated activities with regards to the management system and:

- Is appropriate to the purpose and context of our company including the impact of activities, products and services
- It supports our strategic direction
- It provides a framework for setting our objectives
- It includes a commitment to satisfy applicable requirements including compliance obligations.
- It includes a commitment of continual improvement of the business management system and enhancing performance.

Our Business Management System Manual includes the above policies and a selection of documented processes (process flows) that we deem essential for the effectiveness of the management system, conformance of site services and process in alignment with our strategic direction. Further policies are included as necessary for the success of the business or where we deem it appropriate. We have also included any justification for areas we deem not applicable.

Documentation is subject to control by the Directors or other employees authorised as having authority. The basis of the controls is to ensure that the latest copies, relevant to the accomplishment of site services are available at the time and place of work, to ensure the effective functioning of the company's operations, processes and management system.

Title: Documented Information and GDPR

2 Business Manual

Although it is recognised that there is no requirement for a manual or documented procedure, we have decided that it is in the best interest of the company for a Business Manual to be in place to support:

- training and development including as an induction and promotion tool.
- instruction and direction
- evidence of compliance should complaint / non-conformance be received.
- the tender and pre-qualification questionnaire process
- 3rd party approvals and schemes

The Directors are responsible for the administration, control, maintenance and distribution of the business management system and this Business Management System Manual. The manual will only be issued as directed by the Directors.

There is only one "Controlled" paper copy of the Business Management System Manual. It is also available for all employees of our company. The "master" is subject to periodic back-up.

Uncontrolled copies can be issued to selected Clients or organisations.

Reviews and revisions are listed at the bottom of each section in the table beneath the heading 'Revision'. The Directors are responsible for updating and approving the '**Master Controlled**' copy prior to issue to employees to ensure that they are aware of changes.

No revisions will be made to the manual without the consent of the Directors.

3 Creating and Updating Information

All documented information is identified and described by title, date and author. Reference numbers will also be utilised where beneficial. It will be in accordance with the directives of the General Data Protection Regulations.

Format and media will be electronic or paper to suit effectiveness and suitability (language, graphics, software version). It will be encrypted and restricted to maintain security and will be fit for purpose, easy to understand, unambiguous, relevant and ready retrievable as necessary or upon request. It will be reviewed for suitability and adequacy before being processed, stored, issued or released by those authorised to do so.

Electronic versions are subject to the same controls as those in paper format. They will be maintained in a version that is recognised by the operating software to enable all those who need to, to have access to the current and approved record. Password restriction for reading and / or modification will prevent unauthorised access, processing, change and use.

4 Control of Documented Information.

All documentation essential to the accomplishment of work is controlled and the process is located at the end of this section. All process flowcharts, master records and business manual sections are reviewed for adequacy and suitability during internal audit, at regular department meetings and annually at management review.

The flowchart that follows has been established defining the controls to:

- Approve documents for adequacy and suitability prior to being approved for issue by authorised personnel.
- Review, update and re-approve documents
- Ensure changes and current issue status of documents is identified and available at point of use
- Ensure that documents from external origin being required for planning and operation of the management system are identified and their distribution controlled.

Title: Documented Information and GDPR

Documentation subject to control comprises those detailed documents which are essential to planning, conducting and completing site works, statutory, contractual and business improvement, strategy and business continuity, preventive maintenance, purchasing, measuring and monitoring, analysis & improvement, contracts, administration control, communication, policy, objectives and targets, emergency plans & site requirements, codes of practice and 3rd party schemes, training requirements and competence records, register of significant environmental aspects, risk assessment and hazard control.

All changes to documented information are in writing and are processed to ensure prompt action at the specified point. Changes to documents are reviewed by the same department that performed the original review i.e., author (where possible). However, approval for the issue of changes must be obtained from the Director / authorised deputy. The Director distributes documented information as appropriate to ensure that it is available and suitable for use, when and when it is needed.

Records are introduced to the business management system as an initial issue i.e., issue 1. Subsequent updates or amendment to a document / software programme is controlled by authorised person whereby, following review and subsequent approval by the Director / authorised deputy, it is allocated issue 2; then issue 3 and so on depending upon the number of amendments made to it. Control is either through recording on the actual document (eg approval and issue status at end of the policy and procedure) or through listing on the relevant index signed off as issue and approval by authorised persons within the business

Documented information submitted from external origin and necessary for the planning and operation of the management system are identified and are also subject to recording, maintenance and control. They are issued as necessary within the planning and operation stages to those workers requiring them. Once again, those superseded are identified as such when updates or amendments are received. Outsource arrangement services are likewise required to provide objective evidence of compliance with quality, contractual and statutory requirements.

They demonstrate our achievements in effective operation of the business management system and as evidence of conformity to requirements. They are protected from unintended alteration.

Where appropriate, all obsolete documents are identified and removed from the place of issue to discourage further use. Those, which need to be retained are marked as **'Superseded'** or a line put through it to signify this.

Documented information will always be legible, identifiable, regularly maintained and traceable, and will be made available to those having authority, for ready retrieval and use. Access to records will be restricted to authorised persons. Whether considered **"LIVE"** or **"ARCHIVE"**, they will be collated within a package identifiable to the subject matter or traceable to unique name / number. At all times they will be protected against damage, loss and deterioration. Loss can include loss of integrity, loss of confidentiality and improper use.

Retention periods for documented information is commensurate with the timescales we have deemed appropriate through our mapping exercise under the GDPR regulations and to meet statute for inspection and test records. Records associated with the management system without sensitive or personal information, is normally five years unless there is a legal or contractual requirement to retain beyond this period (e.g. financial records 6 + current year). The Forms Register identifies retention period. It is signed by the Director / authorised deputy to signify that approval for a change in records has been approved. Retention storage shall be restricted to the designated area within the building, which has been allocated for that purpose or if electronic, in folders identified to archive records. Designation is dependent upon the subject matter and the potential of having to retrieve them at a later date.

Disposal of documented information is through approved supplier with those of a sensitive nature being shredded / torn prior to disposal or a confidential disposal agent utilised supported by a Certificate of Destruction for each disposal.

Title: Documented Information and GDPR

5 Use and Access

Access to personal data is strictly limited to authorised employees, contractors, and service providers who require such access for legitimate business purposes and who are bound by confidentiality obligations. Users are granted access based on role-specific permissions, ensuring that individuals can only view, use, or modify the information necessary for their duties. Personal data must not be accessed, shared, copied, downloaded, or transferred without proper authorisation. All access to company systems containing personal information is monitored and may be audited to ensure compliance with UK GDPR and internal security policies. Employees are required to use secure passwords, approved devices, and company-authorised systems when handling personal data. Any suspected unauthorised access, data breach, or misuse of information must be reported immediately to management or the designated Data Protection Officer. Failure to comply with these requirements may result in disciplinary action and, where applicable, legal consequences under the UK GDPR and Data Protection Act 2018

Signed for and on Behalf of Tricore Technical Services Limited

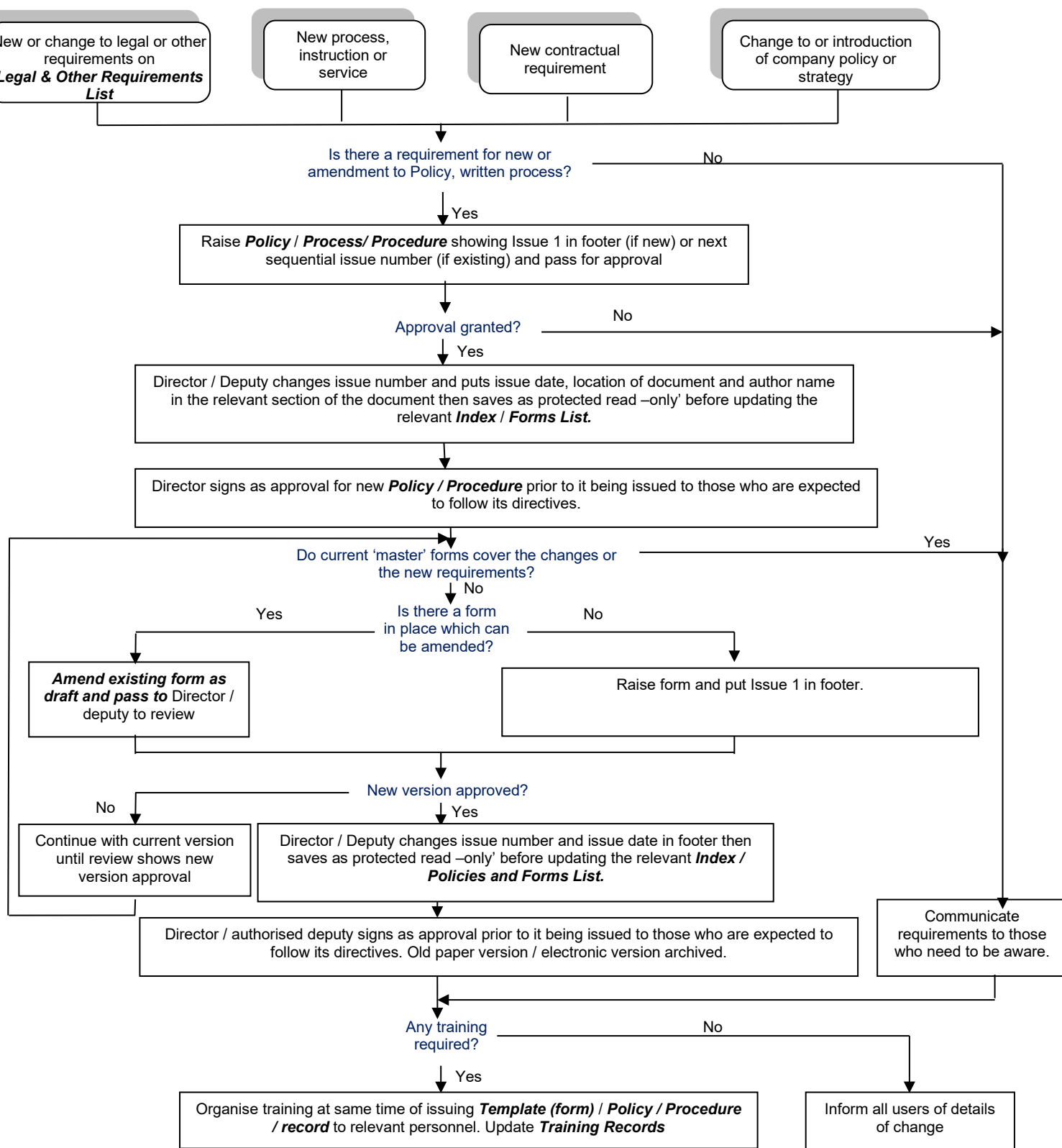


Director P.Bass

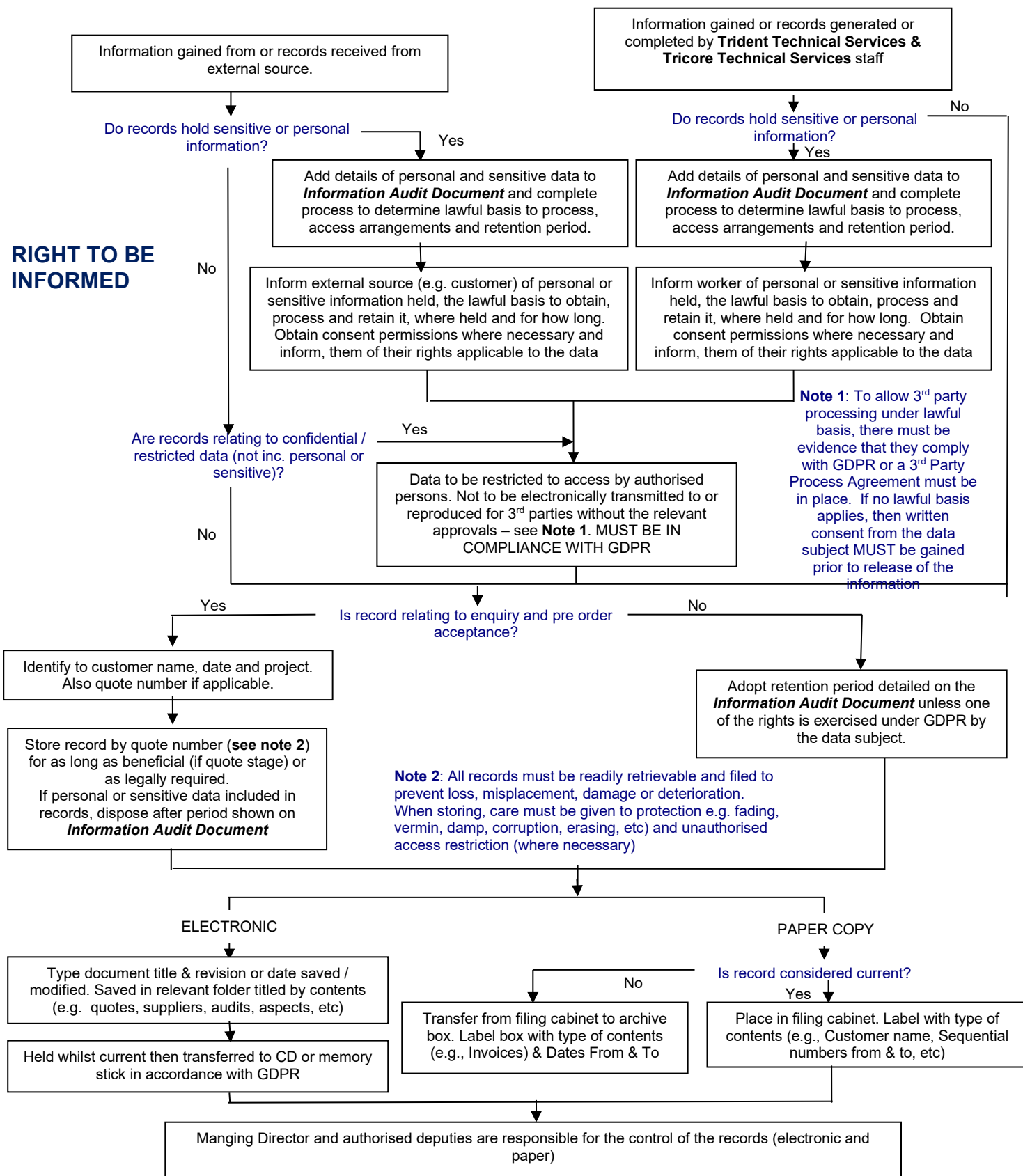
Date: 9/1/2026

Title: Documented Information and GDPR

Procedure



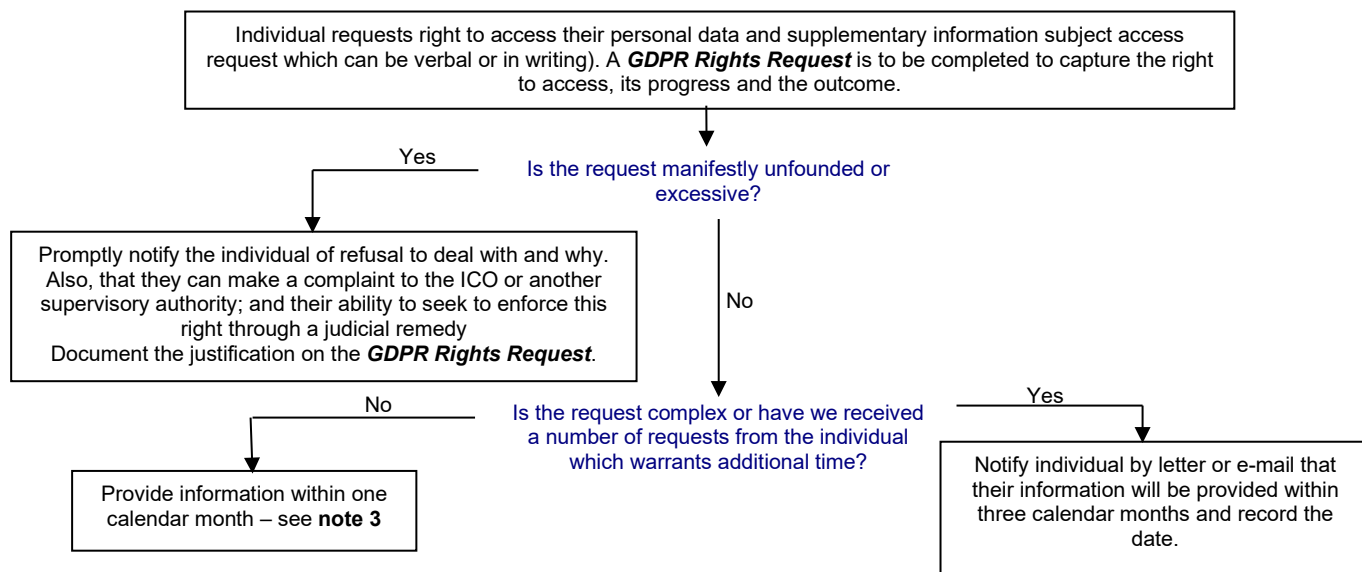
Title: Documented Information and GDPR



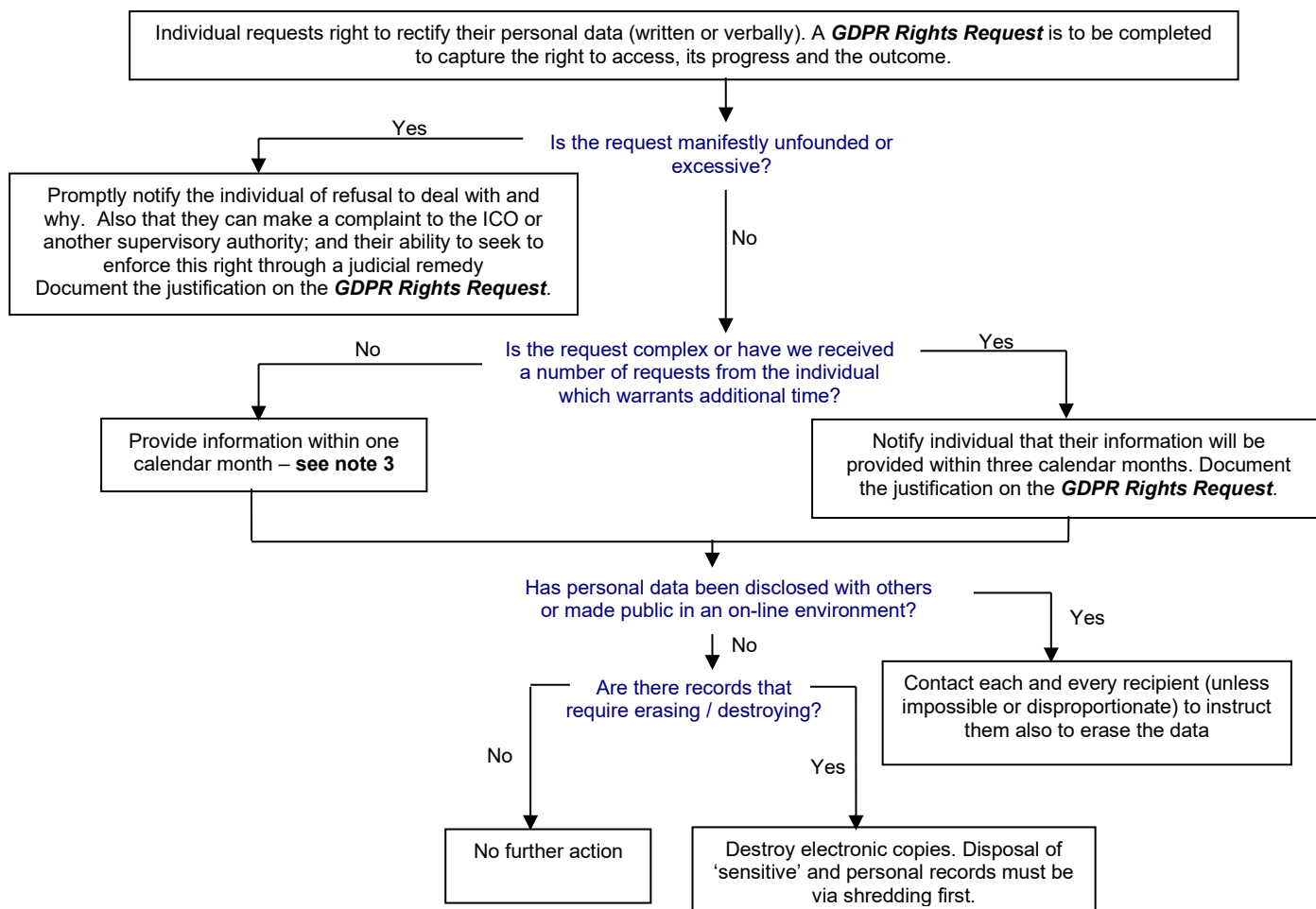
RIGHT TO ACCESS

Note 3. Information provided to an individual will be in a concise, transparent, intelligible and easily accessible form, using clear and plain

Title: Documented Information and GDPR



RIGHT TO RECTIFY



RIGHT TO ERASURE

Title: Documented Information and GDPR

Individual requests right to erasure (right to be forgotten) A **GDPR Rights Request** is to be completed to capture the right to access, its progress and the outcome.

Note 4: Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

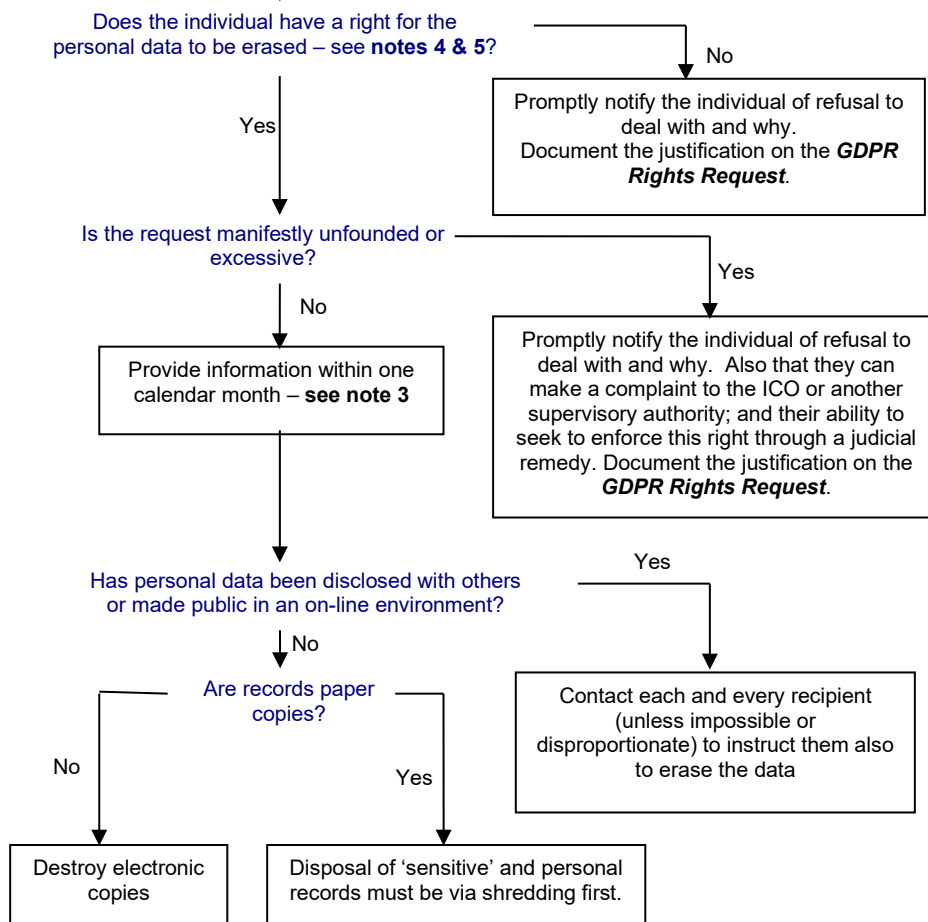
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Note 5: Refusal to comply with a request for erasure is warranted where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims

and for special category information:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).



Title: Documented Information and GDPR

RIGHT TO RESTRICT

Note6. Right to restrict processing applies if:

- the individual contests the accuracy of their personal data and we are verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual

Individual requests right to restrict personal data. A **GDPR Rights Request** is to be completed to capture the right to access, its progress and the outcome.

Is there sufficient reason to investigate whether the individual has a right for the personal data to be restricted –

No

Promptly notify the individual that there is no right to restrict processing and why. Document the justification on the **GDPR Rights Request**.

Yes

No

Is the request manifestly unfounded or excessive?

Provide information within one calendar month – **see note 3**

Promptly notify the individual of refusal to deal with and why. Also that they can make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy. Document the justification on the **GDPR Rights Request**.

Either:

- temporarily move the data to another processing system; OR
- make the data unavailable to users; OR
- temporarily remove published data from a website

No

* Do we need to process the data

- for the establishment, exercise or defence of legal claims;
- for the protection of the rights of another person (natural or legal); or
- for reasons of important public interest?

Yes

Is the restriction relating to?

- the individual disputing the accuracy of the personal data and we are investigating this; or
- the individual is objecting to us processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of our legitimate interests, and we are considering whether your legitimate grounds override those of the individual?

No

Yes

Decision made whether restriction can be lifted i.e. accuracy of the data, or whether our legitimate grounds override those of the individual.

No

Can we lift the restriction?

Yes

Data to be stored in restricted folder with access to authorised persons within the business only. **Cannot process unless consent given by data subject.**
* also, the 3 reasons above could apply at any time after restriction in place

Notify data subject that we intend to lift the restriction on the basis that data accurate or that our legitimate grounds override theirs and the reason for refusal to act under their right to rectification and right to object. Also that they can make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy. Document the justification on the **GDPR Rights Request**.

Has personal data been disclosed with others or made public in an on-line environment?

No

No further action required

Yes

Contact each and every recipient (unless impossible or disproportionate) to instruct them also to erase the data

Title: Documented Information and GDPR

6 GDPR

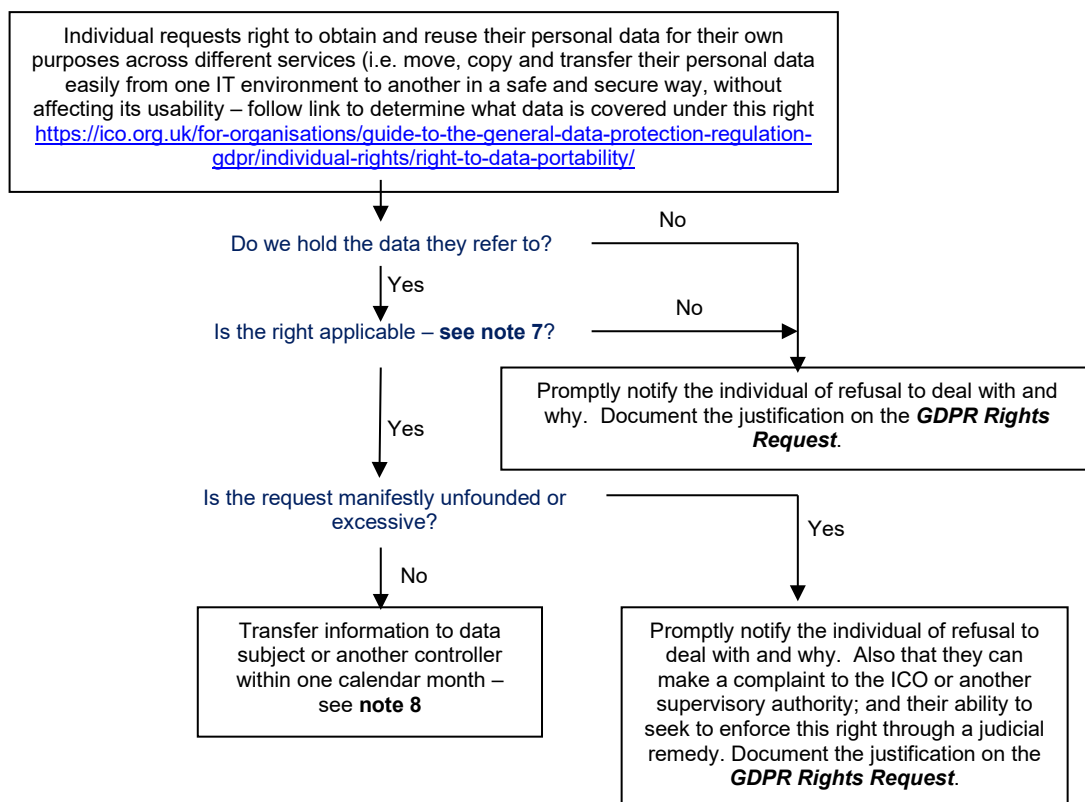
RIGHT TO DATA PORTABILITY

Note 7: The right to data portability only applies when

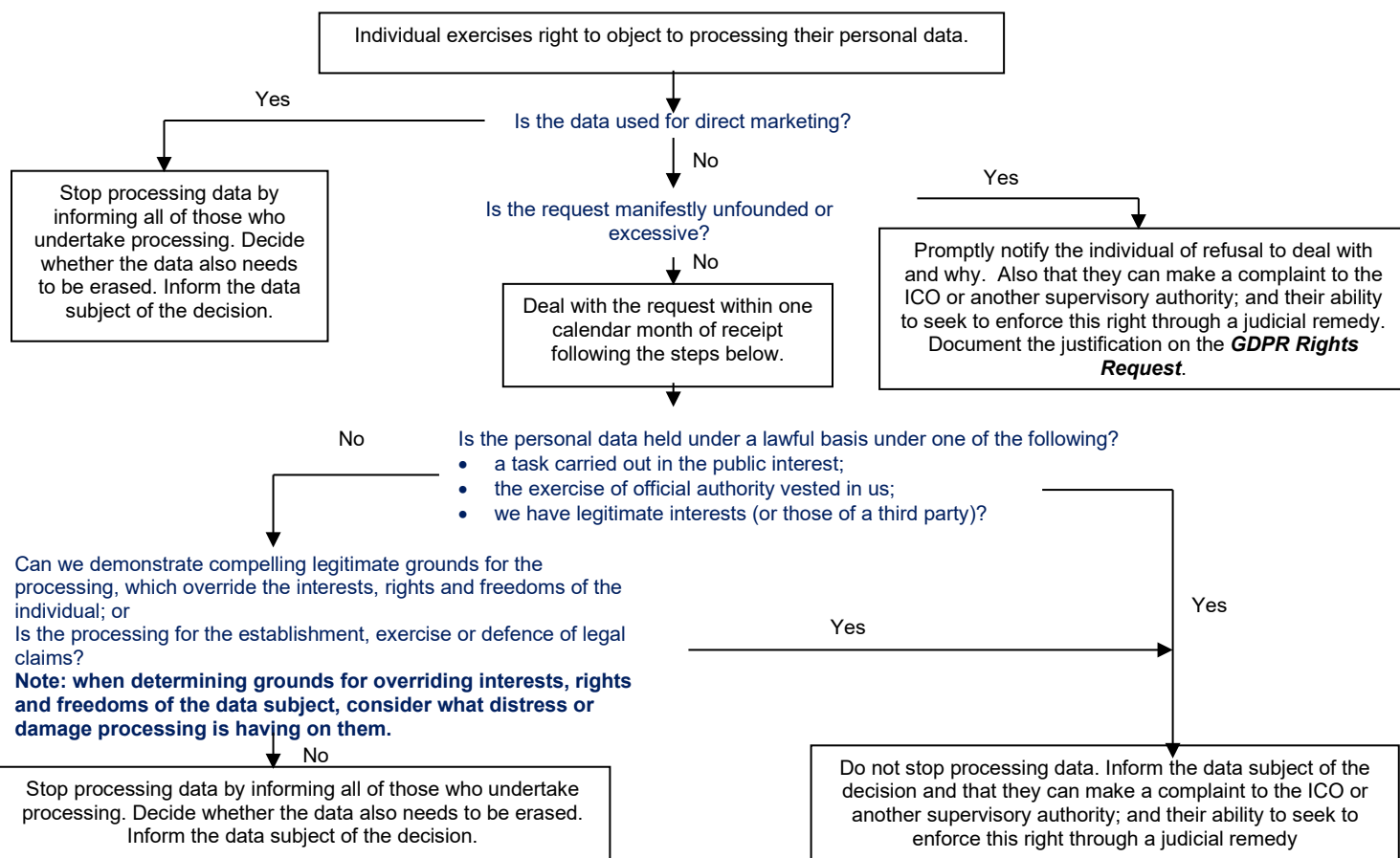
- consent has been used for the lawful basis for processing this information **or** it is applicable to the performance of a contract; and
- you are carrying out the processing by automated means (i.e. excluding paper files)

Note 8. information provided through data portability request will be provided in a format that is:

- structured;
- commonly used; and
- machine-readable.

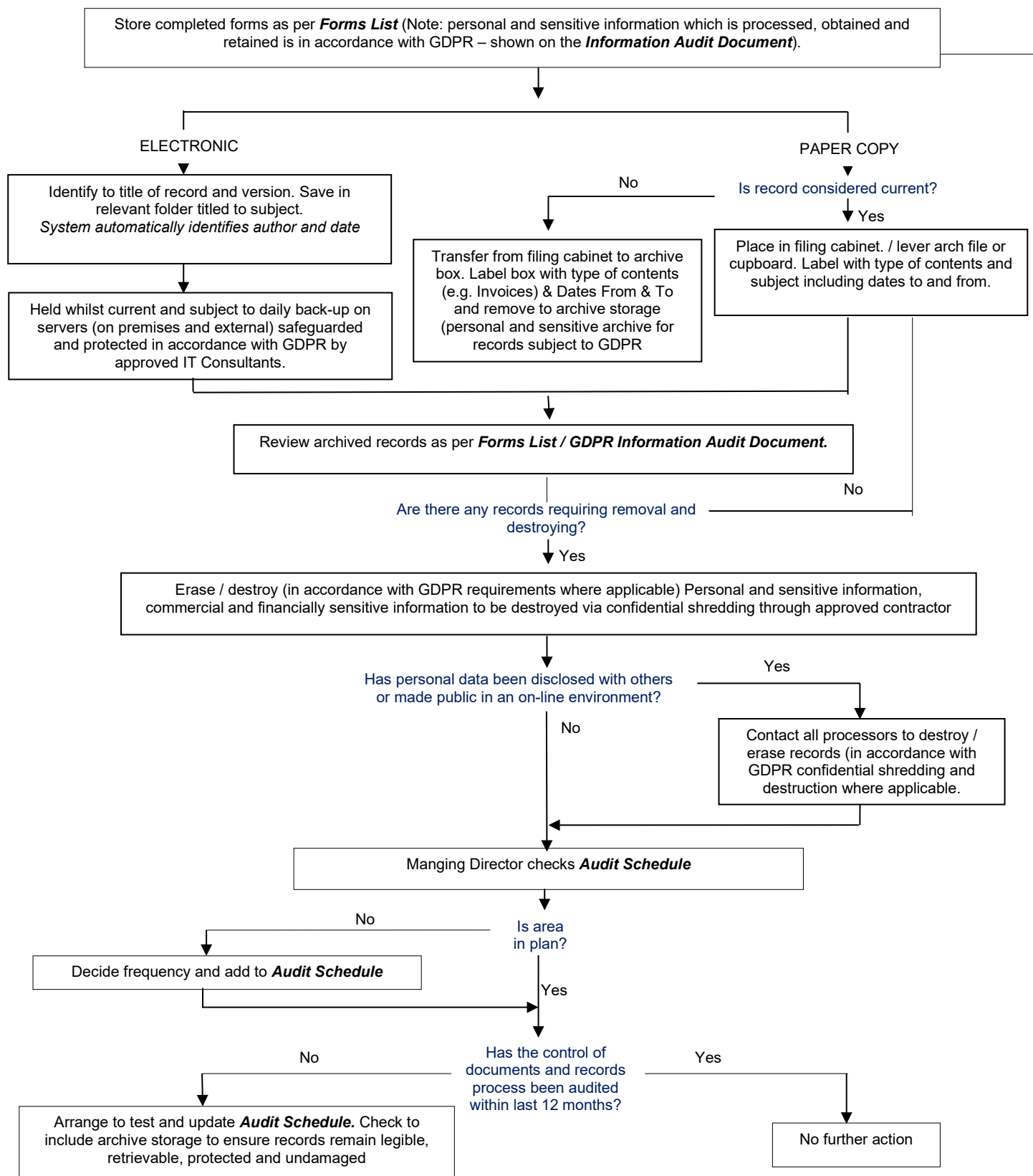


RIGHT TO OBJECT



Storing, Archiving & Disposal

Title: Documented Information and GDPR



Appendix 1

What privacy information should we provide to individuals?

The table below summarises the information that we must provide. What we need to tell people differs slightly depending on whether we collect personal data from the individual it relates to or obtain it from another source.

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

Title: Documented Information and GDPR**7 Other References - linked policies and procedures**

There are a number of policies, procedures and documents that should be read in conjunction with this section. They are:

- Data Protection Act and General Data Protection Regulations.

8 Approval, Retention and Issue Details

Document available as read only from the following location:

BUSINESS MANAGEMENT SYSTEM

Review Frequency:

Every 3 years unless statutory, audit, incident or non-compliance require otherwise

Retention: Controlled printed copies destroyed when superseded. Electronic copy held for 5 years unless statutory required or contractually requested to hold beyond this period.

Issue	Details	Author	Approval	Date
1	Initial Issue	Paul Gordon	Andrew Jones	18/01/2023
2	Tricore Technical Services added to the policy.	Paul Gordon	Andrew Jones	3/10/2023
3	Review Period – Added use and access in line with 2025 update	M Walton	P Bass	9/1/26