# LEGAL SERVICES OPERATIONAL PRIVACY CERTIFICATION SCHEME


March 2023

**LOCS:23 STANDARD V12.2**

2TWENTY4 CONSULTING
DATA PROTECTION SERVICES

# Version Control

| Approved by | Role | Date | Version |
|---|---|---|---|
| T Hyman | Managing Director | Aug 21 | 1.0 |
| T Hyman | Managing Director | Nov 21 | 2.0 |
| T Hyman | Managing Director | Dec 21 | 3.0 |
| T Hyman | Managing Director | Mar 22 | 4.0 |
| T Hyman | Managing Director | May 22 | 5.0 |
| T Hyman | Managing Director | May 22 | 6.0 |
| T Hyman | Managing Director | Sep 22 | 7.0 |
| T Hyman | Managing Director | Sep 22 | 8.0 |
| T Hyman | Managing Director | Oct 22 | 9.0 |
| T Hyman | Managing Director | Jan 23 | 10.1 |
| T Hyman | Managing Director | Jan 23 | 10.2 |
| T Hyman | Manging Director | Mar 23 | 11.0 |
| T Hyman | Managing Director | Mar 23 | 12.0 |
| T Hyman | Managing Director | Mar 23 | 12.1 |
| T Hyman | Managing Director | Oct 23 | 12.2 |



The certification criteria contained within this document have been approved by the Information Commissioner's Office in accordance with the Commissioner's tasks and powers under Articles 57(1)(n) and 58(3)(f) pursuant to Article 42(5) of the UK General Data Protection Regulation.'

# Contents

# 1 Introduction

Legal Service Providers such as Law firms and associated Organisations such as Barrister's Chambers process extremely large amounts of data much of which is Personal Data and often Special Category Data or criminal offence data. Clients of legal services range from 'blue chip' corporations planning a corporate takeover to the general public seeking advice on life activities such as conveyancing, medical claims and will writing. The legal industry relies on a high level of trust between Clients and Legal Service Providers who in turn will trust their own suppliers as personal and special category data is moved around in the 'supply chain'.

In addition, as Legal Service Providers tend to provide a wide range of services to a large number of Clients, the value of the data processed has been recognised by hackers which can be seen in the significant increase in technical attacks including phishing, impostor emails and ransomware.

Over the years, Legal Service Providers have embraced and adopted technology to process and deliver their services to Clients which in turn has seen a significant uptake of 'cloud' infrastructure and software provision. The technology used by Legal Service Providers can be mainstream or bespoke to the industry and is often referred to colloquially as 'Legal Technology'.

One challenge that all Legal Service Providers have is ensuring that the trust relationship they build with their Clients is not let down by the technology services they subscribe to. It is essential that Legal Service Providers select third-party vendors and services that are able to demonstrate and maintain protections for the Client data shared with them.

In the absence of an approved Certification Scheme the users of legal services can only trust that Legal Service Providers are applying required and appropriate protections. In turn the Legal Service Providers can only trust their own suppliers and attempts to ascertain adequacy can be complex, time consuming and expensive. In addition, the Senior Management teams within Legal Service Providers rely on an internal department or person's assurance that the Organisation is 'compliant' with current data protection legislation.

This standard has been developed in response to Client concern, Senior Management feedback, the increasing risk of Personal Data Breach or theft and a general industry desire to ensure the privacy and security of Client personal data when selecting third-party service providers.

**Key benefits of the LOCS:23 Standard**

LOCS:23 is intended to become the 'kite mark' for Legal Service Providers and ensure the following benefits:

**Client Benefits**

- Enhanced trust in knowing their Legal Service Provider has had its Client File Processing certified to UK GDPR standards.
- Confidence that personal data provided will be protected, processed fairly and only kept as long as is necessary.
- Knowledge that the Legal Service Provider has strong information security in place.
- Knowledge that the Organisation recognises Data Subject rights and has the processes to enable them.
- Knowledge that the Legal Service provider's breach response processes have been assessed to confirm they have appropriate management and remediation controls thus ensuring Clients are notified as soon as possible and potential harm is minimised.
- Knowledge that the Legal Service Provider's data sharing processes have been assessed to ensure personal data is only shared where lawful to do so and with the required protections in place.

**Legal Service Provider Benefits**

- Give confidence to users of Legal Services.
- Maintain consistent standards through the legal supply chain.

- Promote Data Protection best practice in Legal Service Providers and their vendors/service providers.
- Reduce time and resource spent on assessing Third Party Data Processors.
- Ensure the territorial scope of UK GDPR is recognised by non-UK Legal Service Providers and their vendors/service providers.
- Assist in meeting Article 28 requirements (where appropriate).
- Certification may act as a recognised 'supplemental measure' for cross border data transfers.

This document defines the LOCS standard and details the minimum criteria that a provider of services to the Legal industry should meet including the technical, organisational and documentary requirements needed to meet the LOCS certification requirements.

The LOCS certification is designed to assist and support any obligation to meet UK GDPR standards.

# 2 Scope

The primary processing activity within the scope of this standard is:

**Processing of Personal Data in the Client File**

Legal Service Providers that process Client data are likely to include in that processing the Personal Data of the Client. Client data including any Personal Data will be kept as a single electronic record of the Client engagement known as the 'Client File'. The Client File may be electronic or physical and may exist in multiple locations. As a consequence, Legal Service Providers must meet UK GDPR requirements particularly in protecting the data and honouring the Client's rights as a Data Subject.

In addition, there are a number of sub-processes that are necessary to maintain the file as listed below in 'Processing Activities in Scope'.

The LOCS:23 standard is applicable to any provider of Legal Services who wish to be LOCS:23 certified and is able to demonstrate their application of Data Protection best practice. The LOCS:23 standard controls are mapped to the UK GDPR requirements relating to the processing in scope to enable certified organisations to demonstrate compliance with UK data protection law (see Appendix 1 and Appendix 2)

Legal Service Providers, and their supplier/Vendors/Solution providers that have demonstrated compliance with the LOCS:23 standard are entitled to use the LOCS:23 logo on their promotional material once certified by a UKAS approved certification body.

**Ensuring protection of Client data when shared**

Legal Service Providers may use Data Processors and/or Sub-Processors in their supply chain to assist with or provide Processing services. Legal Service Providers may also share Client data with other Legal Service Providers or Data Controllers. To ensure complete protection across the Legal Service supply chain, these should be included within scope where applicable.

Legal Service Providers are obliged to ensure the privacy and security of Client Personal Data when selecting and using third-party service providers or sub-processors.

## 2.1 Scope of Certification Scheme Standard

The standard sets out the technical and organisational requirements for activities concerned with the Processing of Personal Data when maintaining Client files including:

- Initial engagement with the Client;

- Due diligence regarding the Client;
- Data Processing, data archival and data destruction as relates to the Client file;
- Technical and organisational measures, including information security management, vulnerability scanning, penetration testing, data privacy, protection and security;
- Client rights, including access to privacy policies, access to information, rights to rectification, erasure, restricting processing, data portability and right to object;
- Internal Governance
- Supply chain sub-contracting of processing activities
- Communicating with Clients

## 2.2 Processing Activities in Scope

To be eligible for certification against the LOCS:23 standard, applicants shall be maintaining Client data files and carrying out one or more of the following data Processing activities as they pertain to the lifecycle of the Personal Data contained within the Client File:

- Collection of Client Personal Data;
- Storage of Client Personal Data whether long term or transient;
- Modification of Client data (for example updating Marketing information);
- Transmission of Client data whether within the UK or cross border;
- Protection of Client data whether long term or transient;
- Destruction of Client data whether paper or electronic

NOTE: When seeking Data Processor certification, the scope applies to any relevant systems or processes that assist the Data Controller with one or more of the above activities.

## 2.3 Types of Organisations in Scope

The scope of the LOCS:23 certification covers any of the following types of Organisation acting as a Data Controller, Data Processor or Sub-processor that is providing any of the Processing activities in 'Processing Activities in scope':

Data Controllers may use Data Processors to assist with the general Processing of Client data.

Data Processors may use Sub-processors to assist with the general Processing of Client data.

Data Controllers within scope

- Law firms
- Solicitors
- Barristers
- Other providers of legal services

Data Processors/Sub-processors within scope

- Software providers
- Software-as-a-service (SAAS) providers
- Infrastructure-as-a-service (IAAS) providers

- Platform-as-a-service (PAAS) providers
- External consultants
- Service Providers (e.g. translation, transcription, off-site storage etc)
- 3rd Party Legal Service Providers (e.g. Barristers, law firms, Notaries etc)

## 2.4 Territorial Scope for LOCS

The LOCS:23 Certification scheme is applicable to where:

- the data Processing activities are conducted by Organisations (controller, joint controller or processor) established in the United Kingdom; or
- the data Processing activities are conducted by Organisations (controller, joint controller or processor) not established in the United Kingdom but relate to the offering of legal services (even if free of charge) to Data Subjects situated in the United Kingdom.

## 2.5 UK GDPR areas out of Scope

The following areas of UK GDPR do not relate to the Processing of Personal Data within the Client File and are therefore not within the scope of this standard:

| | |
|---|---|
| **Article 8** - Conditions applicable to child's consent in relation to information society services | There are no Information Society Services included within the processing of Client Data and no child consent is required. |

## 2.6 Processing areas out of Scope

Any Processing that is not related to the Client File is out of scope.

This will include but is not restricted to:

- Processing of employee data
- Processing of Third Party Supplier data
- Law enforcement processing subject to DPA 2018, Part 3
- Information Society Services

## 2.7 Target of Evaluation

This Standard assesses the protective measures afforded to a Client's Personal Data by Legal Service Providers.

The applicant for LOCS:23 certification will be a Data Controller, Joint Controller or Data Processor who provides legal services to Clients or who provides solutions or services to Legal Service Providers. This may include an Organisation who acts as a sub-processor to an in-scope Data Processor.

An applicant for LOCS:23 certification will be required to document information related to the Client File processing activities in scope (listed above) being presented for certification including justifying any exceptions (activities to be excluded from the evaluation).

The core components of the Client File Processing are the data provided, the technology used, any Third-Party interactions and any Processing activities during the lifecycle of the file.

The required information will include the following:

| | |
|---|---|
| **Processing lifecycle beginning to end** | e.g. Client inception to Matter closure |
| **Categories of data** | e.g. Contact details, financial details |
| **Special Category data types** | e.g. Medical data, Children's data |
| **Criminal Offence data** | e.g. Criminal records |
| **Location of Processing** | e.g. exclusively UK |
| **Technology Systems/Vendors used** | e.g. Document Management, CRM, Practice Management, Case Management |
| **Sub-Processors used** | e.g. Document Management hosted on third-party (sub-processor) platform, external IT support |
| **Processes** | e.g. Client onboarding, Client due-diligence, |
| **Specific processing activities** | e.g. Automated Decision Making, Profiling, Biometric identification |
| **Define interactions with third-parties and/or any interdependent processing operations and justify them.** | e.g. external translators, Barristers |
| **Document any exclusions and justify them.** | e.g. Data shared with 'other side' legal services |

# 3 Normative References

## 3.1 Legal Provisions

- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679 as it applies in the United Kingdom by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 as amended.

## 3.2 Related National Standards and Guidance

The LOCS:23 Standard shares a number of requirements and is therefore complimentary to the following standards and guidance:

- ISO 27001:13 – Information technology — Security techniques — Information security management systems — Requirements – The ISO 27001:2013 (also known as BS EN 27001:2017) standard provides a framework for an Information Security Management Systems (ISMS) that enables the continued confidentiality, integrity and availability of information.

  See https://www.iso.org/isoiec-27001-information-security.html

- Cyber Essentials – The government backed certification scheme for the application of Information Security

  See https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

- NIST 800-88 – Guidance for Data Deletion.

  See Guidelines for Media Sanitization (nist.gov)

- NIST AES – Guidance for encryption of data.

  See Advanced Encryption Standard (AES) | NIST

## 3.3 ICO Guidance

Records of Processing Activities. https://ico.org.uk/for-Organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/documentation/how-do-we-document-our-processing-activities/#how

Appointing a data protection officer. https://ico.org.uk/for-Organisations/accountability-framework/leadership-and-oversight/whetherto-appoint-a-dpo/

Transfer of data to a third country. https://ico.org.uk/for-Organisations/data-protection-at-the-end-of-the-transition-period/dataprotection-at-the-end-of-the-transition-period/the-gdpr/international-data-transfers/

Privacy notice. https://ico.org.uk/for-Organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/#what2

Data Controller and Data Processor Contracts. https://ico.org.uk/for-Organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/accountability-and-governance/contracts/

The ICO guidance and materials cited here or referred to within the standard are licensed under the Open Government Licence

### 3.4 Other Documents

EDPB – Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679;

EA 1/22 A:2016 – EA Procedure and Criteria For the Evaluation of Conformity Assessment Schemes by EA Accreditation Body Member;

Accountability Framework, published by the UK Information Commissioner's Office;

UK Additional Accreditation Requirements for Certification Bodies;

WP29 – Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679;

WP29 – Guidelines on personal data breach notification under Regulation 2016/679;

WP29 – Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679;

WP29 – Guidelines on Data Protection Officers ('DPOs');

WP29 – Guidelines on the right to data portability;

WP29 – Guidelines on consent under Regulation 2016/679; WP29 – Guidelines on transparency under Regulation 2016/679;

## 4 Definitions

Some of the definitions for the purposes of this standard are directly taken from the UK GDPR.

**'Client'** An individual who makes use of legal services from a Legal Service Provider.

**'Client File'** The physical or electronic collection of Client data relating to services afforded by a Legal Service Provider.

**'Client File data'** The data personal or otherwise that is contained within the Client File.

**'Criminal Offence Data'** means personal data relating to criminal convictions and offences or related security measures. Additional guidance can be found here: Criminal offence data | ICO

**'Data Controller'** means 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 (but see section 6 of the 2018 Act).

**'Data Processor'** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.

**'Data Subject'** means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name.

**'Employee'** For the purposes of LOCS:23 an employee will be viewed as any directly employed personnel or any personnel representing the business and processing client personal data in that capacity.

**'ICO'** means the Information Commissioners Office.

**'Information Commissioner'** The Information Commissioner is the UK's independent regulator for Data Protection and Freedom of Information, with key responsibilities under the Data Protection Act 2018 (DPA) and Freedom of Information Act 2000 (FOIA), as well as a range of other related legislation.

**'Joint Controller'** Where two or more Data Controllers jointly determine the purposes and means of processing the same personal data.

**'Large Scale Processing'** is determined by taking into account the numbers of Data Subjects concerned, the volume of personal data being processed, the range of different data items being processed, the geographical extent of the activity, and the duration or permanence of the processing activity. Further guidance can be found here: ICO DPO guidance

'**Legal Service Provider'** means an Organisation that offers legal services to Clients.

**'Organisation'** means a Legal Service Provider or Legal Service Provider Supplier.

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

**'Personal Data Breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

**'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.

**'Restricted Transfer'** means a transfer of personal data to a separate controller or processor located outside the UK, who is legally distinct from the exporting Organisation.

**'Special Category Data'** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.

**'Sub-Processor'** means where a Data Processor sub-contracts all or some of the processing to another Data Processor.

**'Third Party'** means a natural or legal person, public authority, agency or body other than the Data Subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process Personal Data.

**'Transfer Impact Assessment'** means the review of a cross-border data transfer process to determine any risk and associated supplemental measures to minimise that risk.

**'UK GDPR'** means General Data Protection Regulation (EU) 2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and section 205(4) of the Data Protection Act 2018.

# 5 Compliance Requirements

**LOCS:23** uses the following compliance requirement terms:

| | |
|---|---|
| **SHALL** | this is mandatory to achieve the **LOCS:23** certification. |
| **SHALL NOT** | this is mandatory to achieve the **LOCS:23** certification. |
| **SHOULD** | this is not required to achieve the **LOCS:23** certification but constitutes current best practice. |

# 6 Methodology

The **LOCS:23** standard is based on the internationally recognised PLAN, DO, REVIEW, ACT model and uses a set of key controls, policies, processes and audits to develop a robust and manageable accountability framework for all Client data that the Organisation processes.

The standard has five core control areas:

- **8.1 - Organisation and File Governance**
- **8.2 - Client Rights**
- **8.3 - Operational Privacy**
- **8.4 - Third Party Suppliers & Data Sharing**
- **8.5 - Monitoring & Review**

**The standard uses the following format:**

| CONTROL REFERENCE | This is used to identify each control section |
|---|---|
| **CONTROL OBJECTIVE** | This is the outcome desired from the control's implementation. |
| **CONTROL** | This is the detail of the control applicable. |
| **CONTROL APPLICATION GUIDANCE** | This is practical guidance, notes and comments. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | This section will indicate whether the control equally applies to a Data Processor, does not apply or that a variation exists.<br><br>See summary table in Appendix 3.<br><br>This control does not apply to Data Controllers. |
| **UK GDPR REFERENCE** | This is the UK GDPR Article that the control relates to where applicable. |
| **AUDIT REFERENCE** | This is used to cross reference the Self-Audit Schedule. See template in Appendix 4. |

To ensure a maintained compliance effort, the framework includes a mandatory self-audit program.

# 7 Certification



**LOCS:23 CERTIFICATION**

This must be assessed by a UKAS approved body that has been evaluated against the standards outlined in ISO 17065 and the UKAS additional accreditation requirements. Approved Certification bodies will be published on the ICO website here https://ico.org.uk/for-Organisations/certification-schemes-register/

Both Controllers and Processors can obtain certification.

There are significant benefits to being certified including:

- **The ICO would likely consider certification as a mitigating factor if you followed the scheme requirements and took all reasonable steps to prevent non-compliance.**
- **The certification may be referenced as a 'supplemental measure' for cross-border transfers of data.**
- **You will be presented with a certificate by the UKAS approved assessment body.**
- **Your Organisation will appear in a national public register of LOCS:23 certified bodies.**

For applicant Organisations to achieve LOCS:23 certification, the following steps will apply:

1. **Determine whether the Organisation is certifying as a Data Controller or Data Processor.**
2. **Ensure the Organisation meets the processing criteria defined in the 'Scope' section.**
3. **Download the LOCS:23 documentation from the ICO website.**
4. **Ensure all controls are in place and can be evidenced.**
5. **Engage with a UKAS approved LOCS:23 Certified Assessment Body (CAB).**
6. **Provide evidence that the controls have been met to a satisfactory level.**
7. **Assessment and Certification will be approved by a UKAS approved CAB where scheme criteria have been met.**

# 8. UK GDPR Compliance Standard LOCS:23 Controls

## 8.1 ORGANISATIONAL AND CLIENT FILE GOVERNANCE

This section describes the controls designed to enable Legal Services certification applicants to demonstrate that they have the required governance model for the Client File in place and that all relevant policies are documented and made available to employees.

An Organisation needs an organisational structure for managing data protection and information governance, which provides strong leadership and oversight, clear reporting lines and responsibilities, and effective information flows.

The Board or other highest level of Senior Management that a Legal Services Provider deploys will have overall responsibility for matters regarding the Personal Data on a Client File and the Privacy Council will have oversight of the day-to-day governance requirements.

### 8.1.1 Privacy Council

| CONTROL REFERENCE | LOCS:23:C1 Governance - Privacy Council |
|---|---|
| **CONTROL OBJECTIVE** | To form an internal governance body to oversee Client File data protection. |
| **CONTROL** | **8.1.1.1** The Organisation SHALL create a Privacy Council that will take overall responsibility for data protection activities.<br>**8.1.1.2** The Privacy Council SHALL include the DPO (or equivalent), the most senior IT professional and at least one of the non-IT Senior Management team.<br>**8.1.1.3** The Organisation SHALL maintain a transparent approach to data processing and ensure compliance with transparency obligations. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** The terms of reference for the Privacy Council can be defined by the Organisation and should include overall Data Protection decision making, policy review and audit review.<br>**NB 2.** **8.1.1** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13** |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.1.1** does not apply to Data Processors. |
| **UK GDPR REFERENCE** | Article 5 (2) |
| **AUDIT REFERENCE** | LOCS:23:A1 Privacy Council |

### 8.1.2 Data Protection Officer

| CONTROL REFERENCE | LOCS:23:C2 - DPO |
|---|---|
| **CONTROL OBJECTIVE** | To appoint a single point of contact responsible for day-to-day duties associated with the protection of Client File data. |
| **CONTROL** | **8.1.2.1** The Organisation SHALL determine whether a Data Protection Officer (DPO) is required under the UK GDPR and appoint one if any of the following criteria are met: |

| | |
|---|---|
| | a. the Processing is carried out by a public authority or body, except for courts acting in their judicial capacity;<br>b. the core activities of the controller or the processor consist of Processing operations which, by virtue of their nature, their scope and/ or their purposes, require regular and systematic monitoring of Data Subjects on a large scale (see definitions); or<br>c. the core activities of the controller or the processor consist of Processing on a large scale of special categories of data pursuant to Article 9 UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 UK GDPR.<br>**8.1.2.2** The Organisation SHALL document the decision.<br>**8.1.2.3** If a DPO is not required by legislation the Organisation SHALL either voluntarily appoint a DPO or assign alternative responsibility for Data Protection (see **NB 4**).<br>**8.1.2.4** The Organisation SHOULD make the manager of Data Protection the single point of contact for Data Protection matters within the Organisation.<br>**8.1.2.5** If a DPO is appointed, they SHALL have specific responsibilities in line with Article 39 of the UK GDPR including:<br>a. to inform and advise the Organisation and the employees who carry out Client File data Processing of their obligations pursuant to this standard, the UK GDPR and other relevant laws, such as PECR;<br>b. to monitor compliance with this standard, the UK GDPR, with other domestic law relating to data protection and with the Organisation's data protection policies;<br>c. providing or overseeing awareness-raising and training of staff involved in Client File Processing operations;<br>d. to provide advice when requested as regards the data protection impact assessment and monitor its performance;<br>e. to cooperate with the ICO;<br>f. to act as the contact point for the ICO on issues relating to Processing, including the prior consultation where required for a DPIA (**8.3.2.9**).<br>**8.1.2.6** In addition, a DPO SHALL in line with Article 38:<br>a. have expert knowledge of data protection law and practices;<br>b. report to the highest level of the business;<br>c. operate independently;<br>d. be afforded the authority, support and resources to do their job effectively. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** If an alternative to the DPO is appointed, the Organisation should document the justification for the decision along with a job description outlining his or her duties and responsibilities.<br><br>**NB 2.** **8.1.2.2** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13**<br><br>**NB 3.** The ICO definition of Large Scale Processing can be found here: ICO DPO guidance. |

| | |
|---|---|
| | **NB 4.** Where it is appropriate to appoint an alternative to a DPO this could be one person, multiple people, or a designated 'committee', depending on the size and structure of the organisation |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.1.2** applies equally to Data Processors. |
| **UK GDPR REFERENCE** | Article 5 (2) Articles 37-39 |
| **AUDIT REFERENCE** | LOCS:23:A2 –DPO |

### 8.1.3 ICO Registration and Cooperation

| **CONTROL REFERENCE** | **LOCS:23:C3 - Registration** |
|---|---|
| **CONTROL OBJECTIVE** | Mandatory registration and cooperation with the ICO |
| **CONTROL** | **8.1.3.1** The Organisation SHALL register with the ICO and pay their annual data protection fee, unless they are exempt. In which case the reasons shall be documented.<br>**8.1.3.2** If applicable, the Organisation SHALL register the DPO's details with the ICO.<br>**8.1.3.3** The Organisation and, where applicable, their representatives, SHALL cooperate, on request, with the Information Commissioner in the performance of the Commissioner's tasks. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1**. Registration information here |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.1.3** applies equally to Data Processors. |
| **UK GDPR REFERENCE** | Article 5 (2) |
| **AUDIT REFERENCE** | LOCS:23:A3 – ICO Registration |

### 8.1.4 Data Protection Principles

The Data Protection principles form the fundamental building blocks for protecting Personal Data.

Organisations must apply these core principles to their processing activities in order to meet UK GDPR requirements.

| **CONTROL REFERENCE** | **LOCS:23:C4 - Principles** |
|---|---|
| **CONTROL OBJECTIVES** | To ensure that core Data Protection principles are applied to the processing of Client data. |
| **CONTROL** | **8.1.4.1** Client File data SHALL be processed lawfully, fairly and in a transparent manner in relation to the Data Subject ('lawfulness, fairness and transparency') in line with sections **8.3.4** and **8.2.2**. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1. Lawfulness** – organisations must identify a lawful basis prior to processing personal data. The lawful basis is connected to the purpose for processing and in most cases, the processing must be necessary to achieve that purpose. |

| | |
|---|---|
| | For the processing in scope the lawful basis is typically contract (between the Legal Service Provider and the Client) and the processing must be necessary for the fulfilment of that contract. Additional Processing such as marketing and promotion may also be in the 'legitimate interest' of the Legal Service Provider. It is good practice that once a lawful basis is decided upon and justified it is recorded for each Processing activity in the Record of Processing Activities.<br><br>Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense.<br><br>**NB 2. Fairness** – Organisations should only handle Personal Data in ways that the Client would reasonably expect and not use it in ways that have unjustified adverse effects on them. Consider using the Client engagement process to document and inform of how the Processing may affect the Clients concerned and justify any potential adverse impact.<br><br>**NB 3. Transparency** – In order to demonstrate this, applicants should include relevant information in their privacy notice (see Privacy Notice) In addition, information regarding Processing should be given where possible at the point of data collection for example in the Client engagement process. This will include the intended purposes for Processing the Personal Data; the lawful basis for the Processing, where the Client file will be located, who will be accessing the data and the retention period.<br><br>**NB 4**. Further ICO guidance regarding lawfulness, fairness and transparency can be found here<br><br>**NB 5**. Where Client and/or ex-employee personal data is retained in an 'alumni' database it will be best practice to record this in the ROPA, record the lawful basis (likely to be consent as per **8.3.4.7 – 8.3.4.11**) indicate a retention period and inform the individual. |
| **CONTROL** | **8.1.4.2** Client File Data SHALL be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation') in line with section **8.3.1**.<br>**8.1.4.3** If a new purpose for processing personal data already collected is proposed an Organisation SHALL only go ahead if:<br>a. the new purpose is compatible with the original purpose;<br>b. you get the individual's specific consent for the new purpose; or<br>c. you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.<br>**8.1.4.4** If a new purpose for processing personal data already collected is proposed based on **8.1.4.3 (a)** compatibility, an Organisation SHALL do a compatibility assessment to decide whether the new purpose is compatible with the original purpose. The assessment should take into account: |

| | |
|---|---|
| | a. any link between your original purpose and the new purpose;<br>b. the context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect;<br>c. the nature of the personal data – eg is it particularly sensitive;<br>d. the possible consequences for individuals of the new processing; and<br>e. whether there are appropriate safeguards – e.g. encryption or pseudonymisation. |
| **CONTROL APPLICATION GUIDANCE** | **NB 6.** Only the Client Data necessary for providing the legal services contracted should be collected. It is important that any secondary purposes (such as marketing) are made clear in the Client engagement process.<br><br>**NB 7.** The following purposes will be considered 'compatible' as laid out in **8.1.4.3 (a)**<br><br>a. archiving purposes in the public interest;<br>b. scientific or historical research purposes; and<br>c. statistical purposes.<br><br>**NB 8.** if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the Data Subject, it is likely to be incompatible with the original purpose.<br><br>**NB 9**. Further ICO guidance regarding purpose limitation can be found here |
| **CONTROL** | **8.1.4.5** Client File Data SHALL be all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') in line with section **8.3.1**. Only the Client Data that is needed to complete the contracted service SHALL be collected. |
| **CONTROL APPLICATION GUIDANCE** | **NB 10.** Any surplus data provided by the Client should be deleted as laid out in **8.1.7**.<br><br>**NB 11**. Further ICO guidance regarding data minimisation can be found here |
| **CONTROL** | **8.1.4.6** Client File Data SHALL be all accurate and, where necessary, kept up to date and steps will 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 ('accuracy').<br>**8.1.4.7** The Organisation SHOULD provide a self-service mechanism for Data Subjects to assist with maintenance of personal data.<br>**8.1.4.8** Where an Organisation collects opinions as part of the Client Data File, they SHALL make clear that it is an opinion, and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, an Organisation SHOULD also record this fact in order to ensure records are not misleading.<br>**8.1.4.9** In order to ensure that records are not inaccurate or misleading, an Organisation SHALL:<br>a. accurately record the information provided; |

| | |
|---|---|
| | b. accurately record the source of the information;<br>c. take steps to ensure the accuracy of the information; and<br>d. carefully consider any challenges to the accuracy of the information (see **8.2.4**). |
| **CONTROL APPLICATION GUIDANCE** | **NB 12.** It is good practice to periodically confirm with the Client that all Personal Data they have provided held on file is up to date and accurate.<br><br>**NB 13**. Further ICO guidance regarding accuracy can be found here |
| **CONTROL** | **8.1.4.10** Client File Data SHALL 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 are processed ('storage limitation') in line with section **8.1.7**.<br>**8.1.4.11** Retention of Client File Data SHALL be managed in line with the Retention & Destruction Policy outlined at **8.1.7**. |
| **CONTROL APPLICATION GUIDANCE** | **NB 14.** This principle can be managed using the Data Retention Policy and associated Retention Schedule that details the lifespan of Personal Data within the Client file. This is typically applied upon completion or closure of a Client Matter.<br><br>**NB 15**. Further ICO guidance regarding storage limitation can be found here |
| **CONTROL** | **8.1.4.12** Client File Data SHALL be processed in a manner that ensures security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using technical or organisational measures ('integrity and confidentiality') in line with sections **8.3.7** and **8.3.8**. |
| **CONTROL APPLICATION GUIDANCE** | **NB 16.** This principle requires that security both in technical and operational form as laid out in **8.3.7** and **8.3.8** be applied to the Client data file.<br><br>**NB 17**. Further ICO guidance regarding integrity and confidentiality can be found here |
| **CONTROL** | **8.1.4.13** The Organisation SHALL be responsible for, and be able to demonstrate compliance with, all above principles ('accountability'). |
| **CONTROL APPLICATION GUIDANCE** | **NB 18.** Accountability will be achieved by ensuring that documentation and records are kept demonstrating compliance with the above principles. These will include the following:<br>a. Record of Processing Activities (**8.3.3**);<br>b. Data Retention Schedule (**8.1.7**);<br>c. Personal Data Breach logs (**8.3.5**);<br>d. Client Rights Response logs (**8.3.6**);<br>e. Completed DPIAs (**8.3.2**);<br>f. Third-party due diligence checklists (**8.4.3**);<br>g. Third-party Processing Agreements (**8.4.4**);<br>h. Transfer Impact Assessments (**8.4.6**);<br>i. Privacy Notice (**8.2.2**);<br>j. Training Records (**8.3.9**); |

| | |
|---|---|
| | k. Internal Audits (**8.5**).<br><br>**NB 19**. Further ICO guidance regarding accountability can be found here |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.1.4.14** Data Processors SHALL:<br>a. act on the instructions of the controller,<br>b. notify the controller if any of their instructions would lead to a breach of UK data protection laws, and<br>c. assist the controller in meeting their data protection obligations.<br><br>**NB 20**. Data Processors can only process the Personal Data on instructions from a controller (unless otherwise required by law). If a Data Processor acts outside of its instructions or processes for its own purposes, it will step outside the role as a processor, would be in breach of contract and the processing may not be lawful. They also risk regulatory action by the ICO. |
| **UK GDPR REFERENCE** | Article 5 (1) Article 5 (2) |
| **AUDIT REFERENCE** | LOCS:23:A4 – Principles |

### 8.1.5 Data Protection and Information Security Policy

| **CONTROL REFERENCE** | **LOCS:23:C5 – Data Protection and Information Security Policy** |
|---|---|
| **CONTROL OBJECTIVE** | To document and distribute a Data Protection Policy to provide staff with enough direction to understand their roles and responsibilities regarding data protection and information governance. |
| **CONTROL** | **8.1.5.1** The Organisation SHALL have a documented Data Protection Policy. The Data Protection Policy shall cover the following as a minimum:<br>a. Data Protection principles<br>b. The types of Client data processed and the purpose<br>c. How data is collected<br>d. Who data is shared with<br>e. How long data is kept<br>f. How data is protected<br>g. Client File access<br>h. Working remotely<br>i. Sending Client documents securely<br>j. Data classification<br>k. Acceptable use of IT<br>l. Removable devices<br>**8.1.5.2** Unless information security is explicitly covered in the data protection policy, the Organisation SHALL have a documented information security policy. The information security policy shall cover the following as a minimum:<br>a. Access Control<br>b. Encryption<br>c. Asset Control<br>d. Network Security<br>e. Acceptable Use<br>f. Password Management |

| | |
|---|---|
| | g. Incident Management<br>h. Breach Notification<br>i. Email Usage<br>j. Clear Desk and Clear Screen<br>k. Removable Media<br>l. Patch Management<br>m. Documents and Records Control<br>n. Electronic destruction<br>o. Remote working<br>**8.1.5.3** The Organisation SHALL make the Data Protection and information security policies available to all employees.<br>**8.1.5.4** The Organisation SHOULD audit employee awareness of the policies on a regular (at least annual) basis.<br>**8.1.5.5** The Organisation SHALL have policies signed off and reviewed at regular intervals. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** **8.1.5.1** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13**<br>**NB 2.** Current and valid certification to ISO 27001/Cyber Essentials may be accepted as supporting evidence of compliance with **8.1.5.2** in certain circumstances. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.1.5** applies equally to Data Processors |
| **UK GDPR REFERENCE** | Article 5 (1) f Article 5 (2) |
| **AUDIT REFERENCE** | LOCS:23:A5 – Data Policy Document |

### 8.1.6 Business Continuity Plan

| **CONTROL REFERENCE** | **LOCS:23:C6 – BC Policy** |
|---|---|
| **CONTROL OBJECTIVE** | To document how the Client File is protected in the event of a serious incident impacting the live data. |
| **CONTROL** | **8.1.6.1** The Organisation SHALL have a documented Business Continuity Plan.<br>**8.1.6.2** The Organisation SHALL make the Business Continuity Plan available to all employees.<br>**8.1.6.3** The Organisation SHALL regularly test the Business Continuity Plan and document results.<br>**8.1.6.4** The Organisation SHOULD audit employee awareness of the plan.<br>**8.1.6.5** The Business Continuity Plan SHALL include at least the following:<br>a. A list of relevant contacts and contact details<br>b. Detailed list of systems and any associated access mechanisms required to enable Client access to their data.<br>c. Descriptions of disruption scenarios and recommended next step actions for each<br>d. Details of how Client data can be recovered or restored as reflected by backup and restore capabilities (8.3.7.5). |

| | |
|---|---|
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** It is recommended that the Business Continuity Plan covers all scenarios for potential disruption to the Client File. Outcomes should be designed to protect the integrity and availability of Client Personal Data.<br><br>**NB 2.** It is recommended that Information Security or Data Protection training carried out contains a reference to the Business Continuity Plan.<br><br>**NB 3.** It is recommended that periodic reminder notices of the Business Continuity Plan are sent out to all employees.<br><br>**NB 4.** It is recommended that the Business Continuity Plan identifies records that are essential and critical to the continued functioning of the Organisation. |
| **UK GDPR REFERENCE** | Article 5 (1) f |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.1.6** applies equally to Data Processors |
| **AUDIT REFERENCE** | LOCS:23:A6– BC Policy Document |

### 8.1.7 Retention & Destruction Policy

| **CONTROL REFERENCE** | **LOCS:23:C7 – R&D Policy** |
|---|---|
| **CONTROL OBJECTIVE** | To document the length of time Client File data will be retained and the process for its safe destruction when no longer required. |
| **CONTROL** | **8.1.7.1** The Organisation SHALL have a documented Retention & Destruction Policy.<br>**8.1.7.2** The Organisation SHALL make the Retention & Destruction Policy available to all employees.<br>**8.1.7.3** The Organisation SHOULD audit employee awareness of the policy.<br>**8.1.7.4** The Organisation SHALL reference retention periods in the Record of Processing Activities, as laid out in **8.3.3.**<br>**8.1.7.5** The Organisation SHALL allocate responsibility for destroying Client File records in line with the Data Retention and Destruction Policy.<br>**8.1.7.6** The Retention & Destruction Policy SHALL include a Retention Schedule that details retention periods applied to data held within the Client File.<br>**8.1.7.7** The Organisation SHALL implement regular diarised activities to ensure Personal Data is deleted in line with the Data Retention schedule.<br>**8.1.7.8** The retention periods SHALL be further broken down into processing sub-sets of the Client File which may include activities such as 'Client due diligence', 'matter information', 'Client contact data' etc. as each may necessitate different retention periods.<br>**8.1.7.9** The Retention & Destruction Policy SHALL include clear instructions for the disposal of both electronic and hard copy data that has reached its stated retention period as laid out in **8.3.8.4.** |

| | |
|---|---|
| | **8.1.7.10** Where Client File data is archived before reaching its stated retention period, it SHOULD be pseudonymised.<br>**8.1.7.11** Where an Organisation intends to keep Personal Data for archiving purposes in the public interest, scientific or historical research purposes; or statistical purposes. It SHALL<br>a. delete any non-essential personal data<br>b. anonymise or pseudonymise personal data (where possible)<br>c. document this in the Retention Schedule<br>d. make this intention clear to Clients<br>e. document this in the ROPA<br>**8.1.7.12** An Organisation SHALL NOT retain data for research purposes if the processing is likely to cause someone substantial damage or substantial distress.<br>**8.1.7.13** An Organisation SHALL NOT retain data for research purposes if it is carrying out the processing for the purposes of measures or decisions with respect to particular people, unless the research is approved medical research. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** The agreed Retention periods should be added to the ROPA (**8.3.3**).<br><br>**NB 2.** Where Client File data is archived, it is recommended that data is moved to an archival system, for ease of access, destruction and ease of use for exercising Client's rights when requested.<br><br>**NB 3.** When completing a Retention Schedule it is recommended that any statutory retention periods be taken into consideration. (e.g. HMRC salary/benefits requirements)<br><br>**NB 4**. When archiving personal data as per **8.1.7.11**, the primary consideration is to anonymise (see **8.3.7.17**) the data where possible as this will mean data protection legislation no longer applies. If anonymisation is not possible, consideration should be given to pseudonymising (see **8.3.7.18**) the data in which case the data protection legislation will still apply. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.1.7** applies equally to Data Processors taking into account any contractual requirements as laid out in **8.4.4.2 (h)** |
| **UK GDPR REFERENCE** | Article 5 (1) e |
| **AUDIT REFERENCE** | LOCS:23:A7– R&D Policy Document |

## 8.2 DATA SUBJECT RIGHTS

An important component of the processing of a Data Subjects Personal Data is the rights afforded to them. Some rights will be absolute, and others will depend on specific circumstances and context.

An Organisation must demonstrate the ability to provide and honour these rights in order to fulfil their legal obligations, while efficient rights management promotes trust and enhances the Clients and Data Subjects experience.

It is important to note that Individuals other than the client (e.g. named third parties, suppliers etc) may exercise their rights where their information is being processed.

### 8.2.1 Transparency & Communication

| CONTROL REFERENCE | LOCS:23:C8 –Transparency & Communication |
|---|---|
| **CONTROL OBJECTIVE** | To provide the required communication to the Data Subject within required timescales when rights are invoked. |
| **CONTROL** | **8.2.1.1** In all cases, when responding to a Data Subject regarding any matter of their rights the information given SHALL be concise, transparent, intelligible and in an easily accessible form, using clear and plain language.<br>**8.2.1.2** The Organisation SHALL when responding to a Data Subject follow the operational requirements as laid out in **8.3.6.**<br>**8.2.1.3** The Organisation SHALL NOT refuse to act on the request of the Data Subject for exercising his or her rights unless they can demonstrate that it is not in a position to identify the Data Subject.<br>**8.2.1.4** The Organisation SHALL provide information to the Data Subject without undue delay and within one month of receipt of the request. The period may be extended by two further months where necessary, taking into account the complexity and number of the requests.<br>**8.2.1.5** If an extension is necessary, the Organisation SHALL inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay.<br>**8.2.1.6** Where the Data Subject makes the request by electronic means, the information SHALL be provided by electronic means where possible, in commonly used electronic format, unless otherwise requested by the Data Subject.<br>**8.2.1.7** If the Organisation refuses the request of the Data Subject, it SHALL inform the Data Subject without delay (and at the latest within one month) of the reasons for not taking action. An Organisation SHALL also inform the Data Subject about the possibility of lodging a complaint with the Information Commissioner and seeking a judicial remedy.<br>**8.2.1.8** Information provided and any communication and any actions taken SHALL be provided free of charge.<br>**8.2.1.9** Where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Organisation may either:<br>a. charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or |

| | |
|---|---|
| | b. refuse to act on the request.<br>The Organisation SHALL document why they consider the request is manifestly unfounded or excessive.<br>**8.2.1.10** Where the Organisation has reasonable doubts concerning the identity of the natural person making the request they may request the provision of additional information necessary to confirm the identity of the Data Subject. If the Organisation does not hold data enabling the verification of a Data Subject's identity they SHALL give the Data Subject the opportunity to provide such data.<br>**8.2.1.11** Where the Organisation has relied upon an exemption to any Data Subject rights as found in the DPA 2018 Schedules 2-4, they SHALL document their reliance on the specific exemption and the reasoning.<br>**8.2.1.12** The Organisation may charge a reasonable fee when providing further copies of information under right of access.<br>**8.2.1.13** If a self-service portal is unavailable (see **8.2.3.8**) documents SHALL be password protected before being returned by email. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** All rights described in **8.2** may apply to individuals other than the client (e.g. named third parties, suppliers etc) who may exercise their rights where their information is being processed.<br><br>**NB 2.** It is recommended that identity be verified whenever a public email address is used (e.g. Gmail) as it is simple for anyone to setup a public email account to misrepresent another (e.g. johnsmith123@gmail.com) This is particularly important before responding with Special Category Data.<br><br>**NB 3.** Legal Service Providers should avoid overly legal language when presenting responses and must deliver them in a commonly used format such as email, MS Word or PDF. The Data Subject (where identity is proven) also has a right to request responses verbally.<br><br>**NB 4.** Possible exemptions can be found in the DPA 2018 Schedule 2 |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.1.1 – 8.2.1.13** do not apply to Data Processors although see **NB 5.**<br><br>**NB 5**. See also **8.3.6.14** and **8.3.6.15.** |
| **UK GDPR REFERENCE** | Article 11 -12 and Article 23 |
| **AUDIT REFERENCE** | LOCS:23:A8– Transparency & Communication |

### 8.2.2 Right to be informed

| **CONTROL REFERENCE** | **LOCS:23:C9 – Right to be informed** |
|---|---|
| **CONTROL OBJECTIVE** | To be transparent as to the processing of a Data Subject's data and make all relevant information available. |
| **CONTROL** | **8.2.2.1** The Organisation SHALL provide the Data Subject with information about how their Personal Data will be processed. |

| | |
|---|---|
| | **8.2.2.2** To ensure fair and transparent Processing, where the Organisation receives data **directly from the Data Subject** it SHALL provide at the time when Personal Data are obtained:<br>a. the identity and the contact details of the Organisation and, where applicable, of the Organisation's representative;<br>b. the contact details of the Data Protection Officer if one is appointed;<br>c. the purposes of the Processing for which the personal data are intended as well as the legal basis for the processing;<br>d. where the Processing is based on legitimate interests, details of the legitimate interests pursued by the Organisation or by a third party;<br>e. the recipients or categories of recipients of the Personal Data, if any;<br>f. where applicable, the details of transfers of the personal data to any third countries or international organisations;<br>g. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;<br>h. the existence of the right to request from the Organisation access to and rectification or erasure of Personal Data, or restriction of Processing concerning the Data Subject, or to object to processing as well as the right to data portability;<br>i. where the Processing is based on consent the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;<br>j. the right to lodge a complaint with the Information Commissioner ;<br>k. whether the provision of Personal Data is a statutory or contractual requirement, or required in order to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;<br>l. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.<br>**8.2.2.3** To ensure fair and transparent Processing, where the Organisation is processing Data Subject data **not provided by the Data Subject** it SHALL provide:<br>a. the identity and the contact details of the Organisation and, where applicable, of the Organisation's representative;<br>b. the contact details of the Data Protection Officer, or alternative;<br>c. the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;<br>d. the categories of Personal Data concerned; |

e. the recipients or categories of recipients of the Personal Data, if any;
f. where applicable, the details of transfers of the personal data to any third countries or international organisations;
g. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
h. where the Processing is based on legitimate interests, details of the legitimate interests pursued by the Organisation or by a third party;
i. the existence of the right to request from the Organisation access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject and to object to Processing as well as the right to data portability;
j. where Processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;
k. the right to lodge a complaint with the Information Commissioner ;
l. from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;
m. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

**8.2.2.4** Where the Organisation does not receive data directly from the Data Subject it SHALL provide that Processing information as laid out in **8.2.2.3 (a) – (m):**

a. as soon as possible after obtaining the Personal Data, but at the latest within one month,
b. if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or
c. if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

**8.2.2.5** Where the Organisation intends to further process the Personal Data for a purpose other than that for which the Personal Data were obtained, the Organisation SHALL provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information as stated in **8.2.2.2(g) – (l).**

**8.2.2.6** An Organisation SHALL maintain a log of historical privacy notices (or other methods for providing Data Subjects with information regarding Processing of their Personal Data) including documenting the dates and details of any changes to them.

**8.2.2.7** An Organisation SHALL periodically review their privacy notices (or other methods for providing Data Subjects with information regarding Processing of their Personal Data) against their Records of Processing Activities (**8.3.3**).

| | |
|---|---|
| | **8.2.2.8** The Organisation SHALL process all requests received under **8.2.2** as laid out in the criteria in **8.2.1.**<br>**8.2.2.9** Where privacy information is not provided as per **NB 4.** an Organisation SHALL document reasons for not providing the information. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1**. The importance of providing Processing information to Data Subjects is a recurring theme and is also covered in Data Protection principles (transparency).<br>The website Privacy Notice and information provided in the Data Subject engagement process are examples of how this information can be provided.<br><br>**NB 2.** Effective use of the Privacy Notice on your website can form part of your organisations approach to the transparency that UK GDPR requires. For transactions that are not website related alternative means of delivering the information to the Data Subject are required.<br><br>**NB 3.** An Organisation should when providing privacy information to individuals, use a combination of techniques, such as:<br>a. a layered approach for easy navigation;<br>b. dashboards;<br>c. just-in-time notices;<br>d. icons; and<br>e. mobile and smart device functionalities.<br><br>**NB 4.** The above information specified in **8.2.2.2** does not have to be provided where the Data Subject already has that information or in the case of data not provided by the Data Subject (**8.2.2.3)** do not have to be provided where:<br>a. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;<br>b. obtaining or disclosure is expressly laid down by a provision of domestic law which provides measures to protect the data subject's legitimate interests;<br>c. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by domestic law, including a statutory obligation of secrecy.<br><br>**NB 5.** If the transfer as per **8.2.2.2 (f)** or **8.2.2.3 (f)** is not made on the basis of an adequacy decision, an Organisation should give people brief information on the safeguards put in place in accordance with Article 46, 47 or 49 of the UK GDPR and the means to obtain a copy of any safeguards or where they have been made available.<br><br>**NB 6.** Possible exemptions can be found in the DPA 2018 Schedule 2 |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.2.1 – 8.2.2.9** do not apply to Data Processors although see **NB7.**<br><br>**NB 7**. See also **8.3.6.14** and **8.3.6.15.** |

| | |
|---|---|
| **UK GDPR REFERENCE** | Article 13 -14 and Article 23 |
| **AUDIT REFERENCE** | LOCS:23:A9 – Right to Information |

### 8.2.3 Right of Access

| **CONTROL REFERENCE** | **LOCS:23:C10 – Right of access** |
|---|---|
| **CONTROL OBJECTIVE** | To enable the Right of Access and provide the Data Subject with access to their processed Personal Data. |
| **CONTROL** | **8.2.3.1** The Organisation SHALL maintain a process as specified in **8.3.6** to enable the Data Subject's right to obtain from them confirmation as to whether or not Personal Data concerning him or her are being processed, and, where that is the case, a copy of the Personal Data.<br>**8.2.3.2** When responding to the request, alongside any data that is provided, the Organisation SHALL also inform the Data Subject of:<br>a. the purposes of the Processing.<br>b. the categories of Personal Data concerned;<br>c. the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international Organisations;<br>d. where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;<br>e. the existence of the right to request from the controller rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing;<br>f. the right to lodge a complaint with the Information Commissioner (ICO);<br>g. where the Personal Data are not collected from the Data Subject, any available information as to their source;<br>h. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.<br>**8.2.3.3** The Organisation SHALL verify the identity of the Data Subject who requests access, including ID verification as documented in **8.3.6.9**, before providing any Personal Data.<br>**8.2.3.4** Where the request is made by a Third Party on behalf of an individual, the Organisation SHALL require evidence from the Third Party that they are authorised to act on behalf of the individual.<br>**8.2.3.5** The Organisation SHALL ensure that providing a copy of the Personal Data SHALL NOT adversely affect the rights and freedoms of others.<br>**8.2.3.6** The Organisation SHALL process all requests received under **8.2.3** as laid out in the criteria in **8.2.1.** |

| | |
|---|---|
| | **8.2.3.7** When relying on an exemption the Organisation SHALL document the reasoning.<br>**8.2.3.8** When providing information in response to an access request an Organisation SHOULD provide a secure, self-serve portal where individuals can download a copy of their information.<br>**8.2.3.9** If a self-service portal is unavailable documents SHALL be passworded before being returned by email. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** To enable this right for Data Subjects, the Organisation must provide access to Personal Data referring or relating to that individual. Please remember that this only applies to living individuals and not Corporations/entities.<br><br>**NB 2.** The Organisation can request the Data Subject specify the Personal Data/Processing activities to which their request relates to help clarify the request and locate the information.<br><br>**NB 3.** Exemptions can be found in the DPA 2018 Schedule 2. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.3.1 – 8.2.3.9** do not apply to Data Processors although see **NB4.**<br><br>**NB 4**. See also **8.3.6.14** and **8.3.6.15.** |
| **UK GDPR REFERENCE** | Article 15 and Article 23 |
| **AUDIT REFERENCE** | LOCS:23:A10– Right of access |

### 8.2.4 Right to Rectification

| **CONTROL REFERENCE** | **LOCS:23:C11 – Right of Rectification** |
|---|---|
| **CONTROL OBJECTIVE** | To enable the Right of rectification and enable the Data Subject to amend, complete or remedy any incorrect or incomplete Personal Data. |
| **CONTROL** | **8.2.4.1** The Organisation SHALL maintain a process as specified in **8.3.6** to enable the Data Subject's right to request incorrect or inaccurate data be corrected.<br>**8.2.4.2** The Organisation taking into account any evidence provided by the Data Subject SHALL take steps to assess the accuracy of the data and rectify, complete or add a supplementary statement if necessary.<br>**8.2.4.3** If the Organisation is satisfied that the data is accurate, it SHALL explain this to the Data Subject, record the fact that the Data Subject disputes the accuracy of the information and inform them of their right to complain in line with **8.2.1.7.**<br>**8.2.4.4** The Organisation SHALL communicate any rectification carried out to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort.<br>**8.2.4.5** If asked, the Organisation SHALL inform the Data Subject which Third Parties have received the Personal Data.<br>**8.2.4.6** The Organisation SHALL process all requests received under **8.2.4** as laid out in the criteria in **8.2.1.** |

| | |
|---|---|
| | **8.2.4.7** When relying on an exemption the Organisation SHALL document the reasoning. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** An example may be the request to update personal contact details held in a Marketing system.<br><br>**NB 2.** Wherever possible it is recommended that a self-service portal be provided to Data Subjects for the purposes of maintaining their Personal Data.<br><br>**NB 3.** Exemptions can be found in the DPA 2018 Schedule 2. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.4.1 - 8.2.4.7** do not apply to Data Processors although see **NB4.**<br><br>**NB 4**. See also **8.3.6.14** and **8.3.6.15.** |
| **UK GDPR REFERENCE** | Article 16, Article 19 and Article 23 |
| **AUDIT REFERENCE** | LOCS:23:A11– Right of Rectification |

### 8.2.5 Right to Erasure

| **CONTROL REFERENCE** | **LOCS:23:C12 – Right of Erasure** |
|---|---|
| **CONTROL OBJECTIVE** | To enable the Right of Erasure and enable the Data Subject to have Personal Data deleted. |
| **CONTROL** | **8.2.5.1** The Organisation SHALL maintain a process as specified in **8.3.6** to enable the Data Subject's right to request from them the erasure of Personal Data concerning him or her.<br>**8.2.5.2** The Organisation SHALL erase Personal Data without undue delay where one of the circumstances in **NB 1** apply.<br>**8.2.5.3** The Organisation SHALL erase Personal Data from all systems, including backup and archival systems.<br>**8.2.5.4** The Organisation SHALL communicate any erasure of Personal Data to each Data Subject to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort, in which case the Organisation SHALL document the reasons why.<br>**8.2.5.5** The Organisation SHALL inform the Data Subject about those recipients if the Data Subject requests it.<br>**8.2.5.6** Where a Data Subject's Personal Data has been made publicly accessible, the Organisation SHALL inform other controllers that the Data Subject has requested they erase any links to, or copies or replications of, their Personal Data.<br>**8.2.5.7** If the Organisation cannot meet the request to have data erased i.e. if an exemption or derogation applies, or if considered manifestly unfounded or excessive, they SHALL document the reasons why and inform the Data Subject. |

| | |
|---|---|
| | **8.2.5.8** The Organisation SHALL process all requests received under **8.2.5** as laid out in the criteria in **8.2.1.**<br>**8.2.5.9** This right SHALL NOT apply to the extent that Processing is necessary for:<br>a. exercising the right of freedom of expression and information;<br>b. compliance with a legal obligation which requires Processing under domestic law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;<br>c. reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);<br>d. archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that Processing; or<br>e. the establishment, exercise or defence of legal claims. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1**. This is not an absolute right and only applies in the following circumstances:<br>a. the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;<br>b. the Data Subject withdraws consent on which the Processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the Processing;<br>c. the data subject objects to the Processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the Data Subject objects to the Processing pursuant to Article 21(2);<br>d. the Personal Data have been unlawfully processed;<br>e. the Personal Data have to be erased for compliance with a legal obligation under domestic law;<br>f. the Personal Data have been collected in relation to the offer of information society services referred to in Article 8(1).<br><br>**NB 2**. Where data has been erased following a Data Subject request, it is important to log the request so that data is not accidentally restored at a later date in the event data is restored from backup for other reasons.<br><br>**NB 3.** Depending on circumstance and technical mechanisms, it may be that Personal Data on backup systems cannot be immediately erased. It is important in this case to put the backup data 'beyond use', meaning most importantly, that the data is not used for any other purpose. |

| | |
|---|---|
| | **NB 4.** Exemptions can be found in the DPA 2018 Schedule 2 |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.5.1 – 8.2.5.9** do not apply to Data Processors although see **NB5.**<br><br>**NB 5**. See also **8.3.6.14** and **8.3.6.15.** |
| **UK GDPR REFERENCE** | Article 17, Article 19 and Article 23 |
| **AUDIT REFERENCE** | LOCS:23:A12– Right of Erasure |

### 8.2.6 Right to Restriction of Processing

| **CONTROL REFERENCE** | **LOCS:23:C13 – Right to Restriction of Processing** |
|---|---|
| **CONTROL OBJECTIVE** | To enable the Right to Restriction of Processing and enable the Data Subject to have Processing restricted in certain circumstances. |
| **CONTROL** | **8.2.6.1** The Organisation SHALL maintain a process as specified in **8.3.6** to enable the Data Subject's right to request the restriction of Processing.<br>**8.2.6.2** The Organisation SHALL restrict the Processing of data without undue delay where one of the circumstances in **NB 1** apply.<br>**8.2.6.3** The Organisation SHALL communicate any restriction of Processing carried out to each Third Party recipient of said data, unless an exemption applies or this proves impossible or involves disproportionate effort, in which case the Organisation SHALL document the reasons why.<br>**8.2.6.4** The Organisation SHALL inform the Data Subject about those recipients if the Data Subject requests it.<br>**8.2.6.5** The Organisation SHALL NOT process the restricted data in any way except to store it unless:<br>a. they have the consent of the Data Subject;<br>b. it is for the establishment, exercise or defence of legal claims;<br>c. it is for the protection of the rights of another person (natural or legal); or<br>d. it is for reasons of important public interest.<br>**8.2.6.6** A Data Subject who has obtained restriction of Processing SHALL be informed by the Organisation before the restriction of Processing is lifted.<br>**8.2.6.7** The Organisation SHALL process all requests received under **8.2.6** as laid out in the criteria in **8.2.1.**<br>**8.2.6.8** Where processing has been restricted, such personal data SHALL, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. |

| | |
|---|---|
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** This is not an absolute right and only applies in the following circumstances:<br>a. the accuracy of the Personal Data on the Data Subject is contested by the Data Subject, for a period enabling the Organisation to verify the accuracy of the Personal Data;<br>b. the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;<br>c. the Organisation no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;<br>d. the Data Subject has objected to Processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the Organisation override those of the Data Subject.<br><br>**NB 2.** Examples of how to restrict Processing include:<br><br>a. temporarily moving the data to another Processing system;<br>b. making the data unavailable to users; or<br>c. temporarily removing published data from a website.<br><br>**NB 3.** The circumstances for when an Organisation should temporarily restrict Processing include:<br><br>a. the individual has disputed the accuracy of the Personal Data and you are investigating this; or<br>b. the individual has objected to you 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 your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.<br><br>**NB 4.** Further exemptions can be found in the DPA 2018 Schedule 2 |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.6.1 – 8.2.6.8** do not apply to Data Processors although see **NB5.**<br><br>**NB 5**. See also **8.3.6.14** and **8.3.6.15.** |
| **UK GDPR REFERENCE** | Articles 18 -19 and Article 23 |
| **AUDIT REFERENCE** | LOCS:23:A13– Right to Restriction of Processing |

### 8.2.7 Right to Data Portability

| | |
|---|---|
| **CONTROL REFERENCE** | **LOCS:23:C14 – Right to Portability** |
| **CONTROL OBJECTIVE** | To enable the Right to Portability and enable the Data Subject to have data ported to another Organisation. |

| | |
|---|---|
| **CONTROL** | **8.2.7.1** The Organisation SHALL maintain a process as specified in **8.3.6** to enable the Data Subject's right to request that Personal Data be ported.<br>**8.2.7.2** Where the individual has provided data to the Organisation, and the Processing is:<br>a. based on consent or contract; and<br>b. is carried out by automated means,<br>the Organisation SHALL, on request from the Data Subject:<br>c. provide the data to the Data Subject in a structured, commonly used, and machine-readable format; and<br>d. transmit those data without hinderance to another Organisation where technically feasible.<br>**8.2.7.3** The Organisation SHALL process all requests received under **8.2.7** as laid out in the criteria in **8.2.1**.<br>**8.2.7.4** When relying on an exemption the Organisation SHALL document the reasoning. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** The concept of portability is akin to 'switching' as might occur with a mobile phone network provider or personal bank account.<br><br>**NB 2.** The right to portability only applies to data provided by a Data Subject and only to data processed by automated means.<br><br>**NB 3.** A Data Subject may request to have their Personal Data ported to another Legal Service Provider in which case if the request is met the data must be sent securely and in a readable format such as PDF or MS Word.<br><br>**NB 4.** Exemptions can be found in the DPA 2018 Schedule 2 |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.7.1 – 8.2.7.4** do not apply to data Processors although see **NB 5.**<br><br>**NB 5.** See also **8.3.6.14** and **8.3.6.15.** |
| **UK GDPR REFERENCE** | Article 20 and Article 23 |
| **AUDIT REFERENCE** | LOCS:23:A14 – Right to Portability |

### 8.2.8 Right to Object

| **CONTROL REFERENCE** | **LOCS:23:C15 – Right to Object** |
|---|---|
| **CONTROL OBJECTIVE** | To enable the Right to Object and enable the Data Subject to stop their data being processed. |
| **CONTROL** | **8.2.8.1** The Organisation SHALL maintain a process as specified in **8.3.6** to enable the Data Subject's right to object to their personal data being processed.<br>**8.2.8.2** Where the Data Subject has objected to the Processing and the lawful basis is legitimate interests or public task, the Organisation SHALL cease Processing their data unless the following applies: |

| | |
|---|---|
| | a. the Organisation demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or<br>b. the Processing is necessary for the establishment, exercise or defence of legal claims.<br>**8.2.8.3** Where this request is complied with, the Organisation SHALL no longer process the Personal Data.<br>**8.2.8.4** Where an Organisation is Processing a Data Subjects data for direct marketing purposes and a Data Subject objects, the Organisation SHALL cease Processing their data immediately and without question.<br>**8.2.8.5** The Organisation SHALL process all requests received under **8.2.8** as laid out in the criteria in **8.2.1.**<br>**8.2.8.6** Processing SHALL be restricted whilst the objection is being considered.<br>**8.2.8.7** When relying on an exemption the Organisation SHALL document the reasoning. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** Personal Data for direct marketing purposes includes profiling to the extent that it is related to such direct marketing.<br><br>**NB 2.** The Right to Object only applies where legitimate interest or public task are used as the lawful basis for processing Client File Data. This right does not apply to Personal Data processed under the contract lawful basis.<br><br>**NB 3.** Exemptions can be found in the DPA 2018 Schedule 2 |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.8.1 – 8.2.8.7** do not apply to Data Processors although see **NB 4.**<br><br>**NB 4**. See also **8.3.6.14** and **8.3.6.15.** |
| **UK GDPR REFERENCE** | Article 21 and Article 23 |
| **AUDIT REFERENCE** | LOCS:23:A15 - Right to Object |

### 8.2.9 Right not to be subject to automated decision making

| CONTROL REFERENCE | LOCS:23:C16 – Automated Decision Making |
|---|---|
| **CONTROL OBJECTIVE** | To enable the Right to not have automated decision making. |
| **CONTROL** | **8.2.9.1** The Organisation SHALL maintain a process as specified in **8.3.6** to enable the Data Subject's right to NOT be subject to automated decision making.<br>**8.2.9.2** The Organisation SHALL process all requests received under **8.2.9** as laid out in the criteria in **8.2.1**.<br>**8.2.9.3** The Organisation SHALL NOT make decisions about the Data Subject based solely on automated processing, including profiling, which produces legal or similarly significant effects on them.<br><br>This will not apply if the automated decision: |

| | |
|---|---|
| | a. is necessary for entering into, or performance of, a contract between the Data Subject and an Organisation;<br>b. is required or authorised by domestic law which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or<br>c. is based on the Data Subject's explicit consent.<br>**8.2.9.4** If automated decision making is to be used due to one of the above exceptions then an Organisation SHALL:<br>a. offer the right to obtain human intervention;<br>b. enable the Data Subject to express his or her point of view;<br>c. enable the Data Subject to contest the decision. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** Automated Decision Making does not currently have widespread application in Legal Services but the increased use of AI may lead to applications in Data Subject due-diligence. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.2.9.1 – 8.2.9.4** do not apply to Data Processors although see **NB 2**.<br><br>**NB 2**. See also **8.3.6.14** and **8.3.6.15.** |
| **UK GDPR REFERENCE** | Article 22 - 23 |
| **AUDIT REFERENCE** | LOCS:23:A16 – Automated Decision Making |

## 8.3 OPERATIONAL PRIVACY

This section describes the controls designed to enable certification applicants to demonstrate that they are applying the technical and operational controls that ensure Client data will be protected.

### 8.3.1 Data Protection by Design and Default

Data Protection should be integrated into Processing activities and business practices from conception right through the lifecycle. By designing processes and practices with data protection in mind, protecting Client data becomes the default.

| CONTROL REFERENCE | LOCS:23:C17 – Design & Default Privacy |
|---|---|
| **CONTROL OBJECTIVE** | To ensure that data protection is built in to activities relating to the processing of Client File data. |
| **CONTROLS** | **DESIGN**<br>**8.3.1.1** The Organisation SHALL have policies and procedures in place to ensure data protection issues are considered when systems, services, products and business practices involving personal data are designed and implemented.<br>**8.3.1.2** The Organisation SHALL ensure that when developing new IT systems, services, products and processes, that data protection risks are considered, addressed and documented at every stage as laid out in **8.3.2.**<br>**8.3.1.3** The Organisation SHALL ensure that data protection matters are considered and incorporated into new policies or processing that involve processing personal data.<br>**8.3.1.4** The Organisation SHALL, when entering into data transfer or sharing arrangements, ensure that data protection risks are considered, addressed and documented.<br>**8.3.1.5** The Organisation SHALL at the time of designing new processes for maintaining Client File Data, and at the time of the Processing itself, implement technical and organisational safeguards such as pseudonymisation to protect Client Personal Data.<br>**8.3.1.6** The Organisation SHALL design mechanisms into processes that enable implementation of the data protection principles as laid out in **8.1.4.**<br>**8.3.1.7** The Organisation SHALL regularly assess and manage risks, including audit and review of risk assessments.<br>**DEFAULT**<br>**8.3.1.8** The Organisation SHALL implement technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed.<br>**8.3.1.9** The Organisation SHALL restrict by default the amount of Personal Data collected, the extent of any Processing, and the period of storage.<br>**8.3.1.10** The Organisation SHALL ensure that by default access to a Client's Personal Data is restricted to only those that have necessary reason to process that data. |

| | |
|---|---|
| | **8.3.1.11** An Organisation SHALL originally set all software security settings to the highest level of security by default.<br>**8.3.1.12** An Organisation SHALL anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals.<br>**8.3.1.13** An Organisation SHALL only process the Personal Data that it needs for stated purposes(s), and only use the data for those purposes.<br>**8.3.1.14** An Organisation SHALL provide the identity and contact information of those responsible for data protection both within the Organisation and to individuals.<br>**8.3.1.15** An Organisation SHALL adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their Personal Data.<br>**8.3.1.16** An Organisation SHALL offer privacy defaults, user-friendly options and controls, and respect user preferences.<br>**8.3.1.17** An Organisation SHALL only use Data Processors that provide guarantees of their technical and organisational measures for data protection by design.<br>**8.3.1.18** When an Organisation uses other systems, services or products in its Processing activities, it SHALL make sure that it only uses those whose design take data protection issues into account.<br>**8.3.1.19** An Organisation SHALL use one or more privacy-enhancing technologies (PETs) to assist it in complying with its data protection by design obligations.<br>**8.3.1.20** An Organisation SHALL ensure that systems and processes allow intervention in the processing to facilitate Data Subject rights, including the ability to rectify and/or permanently delete data, carry out checks on the system or processes and apply updates and security patches. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** Consider core applications such as the Document Management System and take a 'secure by default' approach (e.g. limiting access to others) only diluting these settings where operationally necessary.<br><br>**NB 2.** Where it is deemed appropriate for all lawyers to have access to Client File Data, all other employees should have access restricted unless operationally necessary.<br><br>**NB 3.** **8.3.1.11 and 8.3.1.16-** Where possible all 'default' settings on software applications that assist with the processing of Client File Data should have the highest security settings and only relaxed for operational requirements.<br><br>**NB 4.** **8.3.1.12** – an example of anticipating risk is keeping aware of current cyber attack trends (e.g. ransomware, targeted phishing etc) and as a result modifying training and/or technical protection. |

| | |
|---|---|
| | **NB 5.** **8.3.1.18** – it is important that when selecting third-party solutions or products, features and options are available to assist in the protection of client data.<br><br>**NB 6.** **8.3.1.19** – for the purposes of this standard, the definition of PET is taken from the European Union Agency for Cybersecurity (ENISA) who refers to PETs as:<br>'software and hardware solutions, i.e. systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.' |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.3.1** applies equally to Data Processors.<br><br>**NB 7. 8.3.1.17** applies to Data Processors in the context of engaging sub-processors. |
| **UK GDPR REFERENCE** | Article 25 |
| **AUDIT REFERENCE** | LOCS:23:A17 – Default Privacy |

### 8.3.2 Risks and Data Protection Impact Assessment (DPIA)

Where it relates to the Client File, it may be that a change to an existing process or an introduction of a new Processing technology is necessary. In such instances an initial risk assessment is required.

The initial risk assessment will determine whether or not a DPIA is required.

If required, a DPIA should consider compliance risks, but also broader risks to the rights and freedoms of Clients, including the potential for any significant social or economic disadvantage should their data be misappropriated. In the event a DPIA is not required it is recommended that the reasons a DPIA has been ruled out is documented.

Successfully embedded within the Organisation the DPIA can be one of the most effective ways to communicate change and enable the DPO or person responsible for data protection to take associated actions such as updating the risk register, updating Processing records and maintaining the Supplier Register.

| **CONTROL REFERENCE** | **LOCS:23:C18 - DPIA** |
|---|---|
| **CONTROL OBJECTIVE** | To ensure that any potential risks to Client File data are assessed when introducing new or modified Processing activities. |
| **CONTROL** | **8.3.2.1** An Organisation SHALL document how they intend to identify, manage and mitigate information risks.<br>**8.3.2.2** An Organisation SHALL have a process for employees and Third Parties to report risks.<br>**8.3.2.3** An Organisation SHALL record risks in a risk register that clearly differentiates information risks.<br>**8.3.2.4** When introducing new or modified Processing activities, the Organisation SHALL carry out an initial risk assessment (see **NB 1** below) to identify any risks to the rights and freedoms of the Client and establish whether a DPIA is required.<br>**8.3.2.5** Where a high risk to a Client's rights and freedoms is possible, an initial risk assessment has identified a |

| | |
|---|---|
| | high risk or where required by the ICO, a DPIA SHALL be completed.<br>**8.3.2.6** An Organisation SHALL provide a DPIA template for internal use.<br>**8.3.2.7** The template SHALL be published and available to all department heads or others that may introduce process change.<br>**8.3.2.8** A DPIA SHALL be completed in particular where the Client File requires:<br>a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated Processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or<br>b. Processing on a large scale of special categories of data referred to in Article 9(1), or of Personal Data relating to criminal convictions and offences referred to in Article 10;<br>**8.3.2.9** If the DPIA indicates that a high risk will be introduced to processing Client File data, the Organisation SHALL mitigate the risk. If this is not possible the Organisation SHALL consult the ICO prior to processing and provide the following information:<br>a. where applicable, the respective responsibilities of the Organisation, Joint Controllers and processors involved in the Processing, in particular for Processing within a group of undertakings;<br>b. the purposes and means of the intended Processing;<br>c. the measures and safeguards provided to protect the rights and freedoms of Clients pursuant to this Regulation;<br>d. where applicable, the contact details of the DPO;<br>e. the data protection impact assessment provided for and;<br>f. any other information requested by the Information Commissioner.<br>**8.3.2.10** The Organisation SHALL seek the advice of the Data Protection Officer, where designated, when carrying out a DPIA.<br>**8.3.2.11** A DPIA SHALL contain as a minimum:<br>a. a systematic description of the Processing operations and the purposes of the Processing;<br>b. an assessment of the necessity and proportionality of the Processing operations in relation to the purposes;<br>c. an assessment of the risks to the rights and freedoms of Clients;<br>d. the risk category of Personal Data;<br>e. abnormal conditions and reasonably foreseeable situations that may lead to Personal Data breaches;<br>f. the measures to address the risks, including safeguards.<br>**8.3.2.12** The Organisation SHALL seek the views of the Client or their representatives on the intended Processing, without prejudice to the protection of commercial or public interests or the security of Processing operations. |

| | |
|---|---|
| | **8.3.2.13** An Organisation SHALL review the DPIA at least annually, or sooner if there is a change of the risk represented by Processing operations.<br>**8.3.2.14** An organisation SHOULD (subject to any confidentiality concerns) publish DPIAs (or a summary of) as a way of being transparent about the processing and any associated risks and how they have been addressed. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1**. Consider how to assess and manage risks where a DPIA is not a requirement. One way to achieve this is to have two forms of DPIA, a Short Form DPIA and a Long Form DPIA. This is particularly useful where the initial risk assessment is not carried out by an individual with strong Data Protection expertise.<br><br>The Short Form DPIA is a basic assessment that includes the following:<br><br>a. What data categories will be processed?<br>b. Where will the data be located?<br>c. Where will the data be processed?<br>d. Who can access the data?<br>e. Will the data be shared?<br>f. How will the data be protected?<br>g. How long will the data be kept?<br><br>The Short Form can be provided to the DPO for all introductions of new Processing or changes to existing Processing. Based on the answers provided to the above questions, the DPO (or equivalent) will assess any associated risks and determine whether a Long Form DPIA is initiated.<br><br>The Long Form DPIA will be laid out as described in **8.3.2.10**.<br><br>**NB 2.** The following process is recommended:<br>a. The stakeholder proposing the process change or new solution initiates the Short Form DPIA and includes as much information as possible.<br>b. The DPO reviews the Short Form DPIA and reverts to the stakeholder with any further questions regarding the proposed Processing. Should the DPO assess that proposed Processing may result in a high risk to the Data Subject, a Long Form DPIA should be requested.<br>c. The DPO documents any potential risks and advises as to remediations indicating any remaining risks.<br>d. The DPO provides the completed DPIA for senior management sign off<br>e. The DPIA is reviewed at pre-determined intervals during the process change lifecycle.<br>An example where a DPIA must be completed – A Legal Service Provider that specialises in Medical Negligence claims has been informed by IT that the Client File hosting platform is to be moved from an internal server to a cloud system based in the US.<br><br>**NB 3**. It is not always apparent from the outset that a 'high risk' will be evident. It is therefore recommended that all proposed changes to Client File processes are communicated |

| | |
|---|---|
| | to the DPO and that a default position be created of always producing a Short Form DPIA unless it is certain that there will not be high risk to Client data.<br><br>**NB 4.** An ICO DPIA template is available here<br><br>**NB 5.** It is recommended that an example DPIA is created with dummy data that will assist the project stakeholders in understanding the information that the DPO will need.<br><br>**NB 6.** **8.3.2.14** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13** |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.3.2.5 – 8.3.2.14** do not apply to Data Processors.<br><br>**8.3.2.15** A Data Processor SHALL have a process in place to identify, document, mitigate and manage information risks.<br>**8.3.2.16** There is no obligation for a Data Processor to complete a DPIA, however a Data Processor SHALL assist a Data Controller with completion of a DPIA as required. |
| **UK GDPR REFERENCE** | Articles 35 - 36 |
| **AUDIT REFERENCE** | LOCS:23:A18 – DPIA |

### 8.3.3 Processing Records

The Record of Processing Activities or ROPA is one of the most important documents in the Organisation's arsenal. A well-constructed ROPA will not only provide the Organisation with a good overview of all business activities, the data processed, who it is shared with and how long it is kept but also acts as a fundamental component of the Organisation's accountability framework as it demonstrates internal discovery to external auditors.

The ROPA should indicate all data Processing activities that relate to the Client File from initial marketing, engagement, due diligence and actual work carried out. This will also include any financial interactions and eventual archiving post matter closure. This will help ensure that the Legal Service Provider understands what data is being processed and is ultimately responsible for that Processing being lawful.

Where an Organisation is acting as a Data Processor there is a slightly different information capture requirement as indicated below.

| **CONTROL REFERENCE** | **LOCS:23:C19 - ROPA** |
|---|---|
| **CONTROL OBJECTIVES** | To document all Processing activities related to the Client File |
| **CONTROL** | **8.3.3.1** The Organisation SHALL document all areas of Processing that involve Personal Data.<br>**8.3.3.2** The Organisation SHALL maintain these records.<br>**8.3.3.3** The ROPA SHALL contain:<br>a. your Organisation's name and contact details, and where applicable, the Joint Controller, their representative and the DPO;<br>b. the purposes of the Processing;<br>c. a description of the categories of individuals and of Personal Data;<br>d. the categories of recipients of Personal Data; |

<table>
<tr><td></td><td>
e. details of transfers to third countries or international organisations, including a record of the transfer mechanism safeguards in place;<br>
f. retention schedules; and<br>
g. a description of the technical and organisational security measures in place.<br>
8.3.3.4 The ROPA SHOULD also contain:<br>
a. The lawful basis for Processing;<br>
b. The IT systems used for Processing Client data;<br>
c. The geographical location of the data and/or the individuals Processing it; and<br>
d. A clear indication of the source of the data.
</td></tr>
<tr><td>CONTROL APPLICATION GUIDANCE</td><td>
NB 1. To prepare a ROPA it is recommended that you:<br>
a. Carry out an information audits using questionnaires for all business departments to find out what Personal Data the Organisation holds;<br>
b. review policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.<br>
NB 2. It is also recommended that as part of an Accountability Framework, the ROPA links to the following:<br>
a. information required for privacy notices;<br>
b. records of any consent used;<br>
c. any controller-controller contracts<br>
d. any controller-processor contracts;<br>
e. Data Protection Impact Assessment reports; and<br>
f. records of Personal Data breaches<br>
g. Any documented Special Category Data processing<br>
h. Any documented Criminal data processing<br>
i. The Data Retention & Destruction Policy<br>
j. The Information Security Policy (8.1.5.2)<br><br>
NB 3. Examples of categories of data include criminal offence, special category and children’s data.<br><br>
NB 4. 8.3.3.1 forms part of an Organisation’s compliance with the principle of accountability described in 8.1.4.13<br><br>
NB 5. The ROPA can cross reference other documentation (such as an Information Security Policy or 27001 compliance documents) to comply with 8.3.3.3 (g)<br><br>
NB 6. To comply with 8.3.3.3 (c) Categories of Data and Categories of Data Subjects must relate to a specific processing activity e.g.<br><br>
<table>
<tr><td>Processing Activity</td><td>Categories of Data Subject</td><td>Categories of Data</td><td>Source of Data</td></tr>
<tr><td>Marketing</td><td>Clients</td><td>Contact Details<br><br>Event preferences</td><td>Provided by Client</td></tr>
</table>
</td></tr>
</table>

| | | | | |
|---|---|---|---|---|
| | | | Dietary Requirements | |
| | | Prospects | Contact Details | Event registration |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.3.3.5** If an Organisation is a Data Processor, **8.3.3.3** is not applicable and instead its ROPA SHALL contain:<br>a. Name and contact details of the processor/s and of each controller on behalf of which the processor is acting, and where applicable, the controller or processor's representative and the DPO;<br>b. Categories of Processing carried out on behalf of each controller;<br>c. details of transfers to third countries, including a record of the transfer mechanism safeguards in place;<br>d. a description of the technical and organisational security measures in place. | | | |
| **UK GDPR REFERENCE** | Article 30 | | | |
| **AUDIT REFERENCE** | LOCS:23:A19 – ROPA | | | |

### 8.3.4 Lawful Processing

For every Processing activity documented in the ROPA a UK GDPR Article 6 lawful basis must be decided upon that justifies that Processing. Where Client Personal Data is Special Category an Organisation must NOT process this data unless a UK GDPR Article 9 condition for Processing is met and is documented. Where Client Personal Data is criminal offence data, an Organisation must NOT process this data unless a condition from Schedule 1 of the UK DPA 2018 is met and documented.

UK GDPR affords 6 options for the lawful Processing of Personal Data. They are of equal standing and the most appropriate option should be decided upon, justified and documented in the ROPA and Privacy Notice.

| **CONTROL REFERENCE** | **LOCS:23:C20 – Lawful Processing** |
|---|---|
| **CONTROL OBJECTIVE** | To determine, justify and document the lawful basis for Processing Client data. |
| **CONTROL** | **8.3.4.1** An Organisation SHALL establish and document a lawful basis from UK GDPR Article 6 before processing begins.<br>**8.3.4.2** The Organisation SHALL NOT process Special Category Data unless one of the UK GDPR Article 9 conditions (see **NB 2.)** for Processing is met and documented.<br>**8.3.4.3** The Organisation SHALL NOT process Criminal Offence Data unless it is either:<br>a. under the control of official authority; or<br>b. authorised by domestic law. This means meeting one of the conditions in Schedule 1 of the DPA 2018.<br>**8.3.4.4** If an Organisation is relying on Article 9 conditions (b), (g), (h), (i) or (j), it SHALL meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018<br>**8.3.4.5** If an Organisation is relying on a condition in Schedule 1 of the DPA 18 to process Special Category Data or Criminal Offence Data as per **8.3.4.4** or **8.3.4.3(b)**, they |

| | |
|---|---|
| | SHALL have an 'appropriate policy document' in place where the condition requires it (see link in **NB 3**.)<br>**8.3.4.6** Where an Organisation relies on an appropriate policy document it SHALL during the relevant period (see **NB 5**)<br>a. retain the appropriate policy document,<br>b. review and (if appropriate) update it from time to time, and<br>c. make it available to the Information Commissioner, on request, without charge. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** The available **Article 6** lawful basis are:<br>a. the Data Subject has given consent to the Processing of his or her Personal Data for one or more specific purposes ('consent');<br>b. Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract ('performance of a contract');<br>c. Processing is necessary for compliance with a legal obligation to which the controller is subject ('legal obligation');<br>d. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person ('vital interest');<br>e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ('public task');<br>f. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child ('legitimate interests').<br><br>**NB 2.** The available **Article 9** Processing conditions are:<br>a. the Data Subject has given explicit consent to the processing of those Personal Data for one or more specified purposes, except where domestic law provides that the prohibition may not be lifted by the Data Subject;<br>b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for safeguards for the fundamental rights and the interests of the Data Subject;<br>c. Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;<br>d. Processing is carried out in the course of its legitimate activities with safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the Processing relates solely to the |

| | |
|---|---|
| | members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;<br>e. Processing relates to Personal Data which are manifestly made public by the Data Subject;<br>f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;<br>g. Processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject domestic law;<br>h. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;<br>i. Processing is necessary for reasons of public interest in the area of public health, such as 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, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy domestic law;<br>j. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.<br><br>**NB 3**. The ICO have produced a template for an 'appropriate policy document' for use with **8.3.4.5** and certain processing under **8.3.4.3** here<br><br>**NB 4**. The most likely conditions for processing Criminal Offence Data, 'legal claims' and 'judicial acts' are described in Schedule 1 of the DPA 2018<br><br>**NB 5.** The DPA 2018 defines 'relevant period' as used in **8.3.4.6** as a period which;<br><br>a. begins when the controller starts to carry out processing of personal data in reliance on that condition, and |

| | |
|---|---|
| | b. ends at the end of the period of 6 months beginning when the controller ceases to carry out such processing.<br><br>**NB 6**. The ICO have produced detailed guidance on the use of special category data here |
| **CONTROL** | **Consent**<br>**8.3.4.7** Where consent is used an Organisation SHALL identify and document why consent is the relevant lawful basis for a Processing activity.<br>**8.3.4.8** Where consent is used an Organisation SHALL present the request for consent in a manner which is clearly distinguishable from any other requests and in an intelligible and easily accessible form, using clear and plain language.<br>**8.3.4.9** Where consent is used, the right to withdraw consent SHALL be afforded and SHALL be as easy to withdraw as it was to give.<br>**8.3.4.10** Where consent is used an Organisation SHALL keep a record of the consent and what privacy information was provided at time of consent.<br>**8.3.4.11** Where consent is used as a lawful basis there are strict requirements for that consent to be valid. Any consent given SHALL be:<br>a. Freely given and not a condition of service;<br>b. Indicated by an affirmative action (no pre-ticked boxes);<br>c. Not linked or combined with any other requirement for consent;<br>d. Fully informed;<br>e. Auditable;<br>f. Separate for each Processing activity. |
| **CONTROL APPLICATION GUIDANCE** | **NB 7.** More advice and guidance on consent can be found here |
| **CONTROL** | **Contract**<br>**8.3.4.12** Where performance of a contract is used an Organisation SHALL identify and document why contract is the most appropriate lawful basis, what contract is being used and how the Processing is necessary for that basis.<br>**8.3.4.13** Where more than one Client contract exists, an Organisation SHALL indicate which contract is being used to justify the use of this lawful basis. |
| **CONTROL APPLICATION GUIDANCE** | **NB 8**. An Organisation can use this lawful basis if:<br><br>a. you have a contract with the Client and you need to process their Personal Data to comply with your obligations under the contract.<br>b. you have a contract with the Client and you need to process their Personal Data so that they can comply with specific counter-obligations under the contract (eg you are processing payment details).<br>**c.** you haven't yet got a contract with the Client, but they have asked you to do something as a first step (eg provide a quote) and you need to process their Personal Data to do what they ask. This applies even if |

| | |
|---|---|
| | they don't actually go on to enter into a contract with you, as long as the Processing was in the context of a potential contract with that individual. |
| **CONTROL** | **Legal Obligation**<br>**8.3.4.14** Where legal obligation is used an Organisation SHALL identify and document why this is the most appropriate lawful basis for a Processing activity by specifying which law is applicable and why the Processing is necessary. |
| **CONTROL APPLICATION GUIDANCE** | **NB 9.** An Organisation can rely on this lawful basis if it needs to process the Personal Data to comply with a common law or statutory obligation.<br>a. This does not apply to contractual obligations.<br>b. The Processing must be necessary. If you can reasonably comply without Processing the personal data, this basis does not apply.<br>c. You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.<br>d. You should be able to either identify the specific legal provision or a source of advice or guidance that clearly sets out your obligation. |
| **CONTROL** | **Vital Interests**<br>**8.3.4.15** Where vital interest is used an Organisation SHALL identify and document why this is the most appropriate lawful basis and how the Processing is necessary for that basis.<br>**8.3.4.16** Where vital interest is used an Organisation SHALL document the specific Client vital interests that require the Processing. |
| **CONTROL APPLICATION GUIDANCE** | **NB 10.** An Organisation is likely to be able to rely on 'vital interests' as its lawful basis if:<br>a. you need to process the Personal Data to protect someone's life.<br>b. The Processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.<br>c. You cannot rely on vital interests for health data or other Special Category Data if the individual is capable of giving consent, even if they refuse their consent.<br><br>**NB 11.** It is unlikely that 'vital interest' will be used as a lawful basis within the context of processing personal data in the Client File as defined in **2.2** |
| **CONTROL** | **Public Task**<br>**8.3.4.17** Where public task is used, an Organisation SHALL identify and document why this is the most appropriate lawful basis for a Processing activity, including specifying the necessary task, function or power, and identifying its statutory or common law basis.<br>**8.3.4.18** Where public task is used, an Organisation SHALL document the public tasks being performed that |

| | |
|---|---|
| | require the Processing and why this processing is necessary. |
| **CONTROL APPLICATION GUIDANCE** | **NB 12.** An Organisation can rely on this lawful basis if it needs to process Personal Data:<br>a. 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or<br>b. to perform a specific task in the public interest that is set out in law.<br>c. It is most relevant to public authorities, but it can apply to any Organisation that exercises official authority or carries out tasks in the public interest.<br>d. You do not need a specific statutory power to process Personal Data, but your underlying task, function or power must have a clear basis in law.<br>e. The Processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.<br><br>**NB 13.** It is unlikely that 'public task' will be used as a lawful basis within the context of processing personal data in the Client File as defined in **2.2** |
| **CONTROL** | **Legitimate Interest**<br>**8.3.4.19** Where Legitimate Interest is used, an Organisation SHALL identify and document why Legitimate Interest is the most appropriate lawful basis and how the Processing activity is necessary for that basis.<br>**8.3.4.20** Where Legitimate Interest is used, an Organisation SHALL document the legitimate interests it will be pursuing and why the Processing is necessary to achieve those interests.<br><br>**8.3.4.21** Where Legitimate Interest is used as a lawful basis the Client SHALL be fully informed as to how their data will be processed. An Organisation SHALL document the specific Legitimate Interests in the privacy notice as laid out in **8.2.2**.<br><br>**8.3.4.22** Where Legitimate Interest is used as a lawful basis for Marketing to the Client they SHALL be given the option to opt-out at the point of contact.<br><br>**8.3.4.23** Where Legitimate Interest is used as a lawful basis an Organisation SHALL carry out a Legitimate Interest Assessment (LIA) prior to processing. A LIA is a three part test where an Organisation needs to:<br>a. Identify a legitimate interest (purpose test);<br>b. Show that the processing is necessary to achieve it (necessity test); and<br>c. Balance it against the Client's interests, rights and freedoms (balancing test).<br><br>**8.3.4.24** The LIA SHALL include a 'balancing test' to show how your Organisation determines that its legitimate interests override the individuals' and considers the following: |

<table>
<tr><td></td><td>a. Protect the interests of vulnerable groups such as people with learning disabilities or children;<br>b. Introduce safeguards to reduce any potentially negative impact;<br>c. Offer an opt-out;<br>d. Determine whether a DPIA is needed;<br>e. Document the decision and the assessment;<br>f. Keep the LIA under review and refresh it if changes affect the outcome.</td></tr>
<tr><td>CONTROL APPLICATION GUIDANCE</td><td>NB 14. Legitimate Interest can be an Organisation's own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.<br><br>NB 15. The 'balancing test' indicated in 8.3.4.23 (c) will fail if the Data Subject would not reasonably expect the processing, or if it would cause unjustified harm, in which case their interests are likely to override the Organisation's legitimate interests."<br><br>NB 16. Where a new purpose for processing personal data is proposed, an Organisation may be able to continue processing for that new purpose on the basis of legitimate interests as long as the new purpose is compatible with the original purpose. For further information as to determining compatibility of processing see 8.1.4.4<br><br>NB 17, The ICO have produced general guidance on the use of Legitimate Interest here<br><br>NB 18. The ICO have produced guidance on the Legitimate Interest Assessment including a LIA template here</td></tr>
<tr><td>CONTROL</td><td>8.3.4.25 An Organisation SHOULD make reference in the ROPA (see 8.3.3) to the lawful basis selected for each Processing activity.</td></tr>
<tr><td>CONTROL APPLICATION GUIDANCE</td><td>NB 15. Example uses of Lawful Basis<br><table><tr><td>Contract</td><td>General Client advice</td></tr><tr><td>Legitimate Interest</td><td>Informing the client of related seminars/publications</td></tr><tr><td>Legal Obligation</td><td>Collecting due diligence data</td></tr><tr><td>Vital Interests</td><td>Unlikely to be used</td></tr><tr><td>Public Interest</td><td>Unlikely to be used</td></tr></table></td></tr>
<tr><td>DATA PROCESSOR ALTERNATIVE CONTROL</td><td>8.3.4 does not apply to Data Processors.</td></tr>
<tr><td>UK GDPR REFERENCE</td><td>Article 6 - 7 Article 9 - 10</td></tr>
<tr><td>AUDIT REFERENCE</td><td>LOCS:23:A20 – Lawful Processing</td></tr>
</table>

### 8.3.5 Personal Data Breach Management

| CONTROL REFERENCE | LOCS:23:C21 –Personal Data Breach Management |
|---|---|
| **CONTROL OBJECTIVE** | To ensure that any breach to the confidentiality, integrity or availability of Data Subject data is managed. |
| **CONTROL** | **8.3.5.1** An Organisation SHALL have a defined and internally published Personal Data Breach reporting process.<br>**8.3.5.2** An Organisation SHALL make all employees aware of the Personal Data Breach reporting process.<br>**8.3.5.3** An Organisation SHALL report 'material' Personal Data Breaches, (as defined in **NB 2**), to the ICO within 72 hours from being made aware unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.<br>**8.3.5.4** Where an Organisation reports a Personal Data Breach after the 72 hour period, the report SHALL be accompanied by reasons for the delay<br>**8.3.5.5** An Organisation SHALL report a high risk Personal Data Breach, as defined in **NB 3**, to the impacted Client without undue delay.<br>**8.3.5.6** An Organisation SHALL maintain a register of all Personal Data Breaches (reportable, non-reportable and any near misses that the Organisation is made aware of.).<br>**8.3.5.7** An Organisation SHALL collect and record the following information for reported Personal Data Breaches:<br>a. The date and time the Personal Data Breach was made known to the Organisation;<br>b. The date and time the Personal Data Breach occurred;<br>c. The name of the individual or supplier reporting the Personal Data Breach;<br>d. The nature of the Personal Data Breach;<br>e. The categories and approximate number of Data Subjects concerned;<br>f. The categories and approximate number of data records concerned;<br>g. Description of the likely consequences of the Personal Data Breach;<br>h. Description of the measures taken or proposed to be taken by the controller to address the Personal Data Breach, including measures to mitigate its possible adverse effects.<br>**8.3.5.8** An Organisation SHALL investigate what led to the Personal Data Breach or near miss occurring (root cause analysis) and implement any measures necessary to prevent reoccurrence.<br>**8.3.5.9** If the ICO are informed of a Personal Data Breach, the following information SHALL be provided:<br>a. a description of the nature of the Personal Data Breach including, where possible:<br>b. the categories and approximate number of Clients concerned;<br>c. the categories and approximate number of Personal Data records concerned;<br>d. the name and contact details of the DPO or other contact point where more information can be obtained;<br>e. a description of the likely consequences of the Personal Data Breach; and |

| | |
|---|---|
| | f. a description of the measures taken, or proposed to be taken, to deal with the Personal Data Breach and the measures taken to mitigate any possible adverse effects.<br>**8.3.5.10** If an affected Data Subject is informed of a Personal Data Breach, the following information SHALL be provided:<br>g. the name and contact details of the Organisations DPO, or other contact point where more information can be obtained;<br>h. a description of the likely consequences of the Personal Data Breach;<br>i. a description of the measures taken or proposed to deal with the Personal Data Breach and a description of the measures taken to mitigate any possible adverse effects;<br>j. The fact that they have the right to raise a complaint to the ICO;<br>k. Potential mitigation activities., and<br>l. Useful links to 'next step' information or organisations.<br>**8.3.5.11** Where an Organisation does not report a Personal Data Breach due to a disproportionate effort (**NB 5**. (c)), they SHALL instead make a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1. Personal Data Breach Definition**<br>There are three types of Personal Data Breach. All must be reported immediately to the Data Protection Officer.<br>a. Confidentiality Breach –where there has been unauthorized access to Client File Personal Data (e.g. lost or stolen device, misused password or hacked system).<br>b. Integrity Breach –where Client File Personal Data has not been lost but is not useable in the current format (e.g. corrupted hard disk).<br>c. Availability Breach - where Client File Personal Data has not been lost and is not corrupt but unavailable to access (e.g. an IT system hosting the data is down).<br><br>**NB 2. Reporting a 'material' breach to the ICO**<br>When a Personal Data Breach has occurred, the DPO needs to establish the likelihood of the risk to the Data Subject's rights and freedoms. If a risk is likely, it is a 'material' breach and the ICO must be notified; if a risk is unlikely, it does not have to be reported. Both reportable and non-reportable breaches must be logged in the Personal Data Breach register.<br><br>**NB 3.** Where, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.<br><br>**NB 4. Reporting a Personal Data Breach to the Data Subject**<br>If a Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subject, the UK GDPR says you must inform those concerned directly and without undue delay (asap). As the definition is 'high' risk this reporting has a higher threshold than ICO reporting. |

| | |
|---|---|
| | **NB 5. Circumstances where a Personal Data Breach does NOT have to be reported to the Data Subject.**<br>The communication to the Data Subject referred to in **NB 4**.is not required if any of the following conditions are met:<br>a. the Organisation has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the Personal Data Breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;<br>b. the Organisation has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise;<br>c. it would involve disproportionate effort.<br><br>**NB 6. Example Breach Reporting Process**<br>a. All personnel must report a Personal Data Breach to the designated person immediately they become aware of the Personal Data Breach.<br>b. A completed Personal Data Breach Form should accompany or follow soon after the report of a Personal Data Breach. The Personal Data Breach Form should be made readily available and can be requested from the DPO (or equivalent).<br>c. The DPO will confirm receipt of the report and log in the Personal Data Breach Register.<br>d. The DPO will determine whether the Personal Data Breach needs to be reported to the Privacy Council and/or the ICO.<br>e. The DPO will determine whether the Personal Data Breach is reportable to the Client(s) impacted.<br>f. The DPO will make reports to d and e.<br><br>**NB 7. Reporting a 'material' Personal Data Breach to the ICO - examples**<br>An example of a reportable Personal Data Breach – An unprotected spreadsheet containing a Clients Medical claim details has been sent to a BCC list of multiple recipients.<br>An example of a non-reportable breach – A memory stick containing multiple Client's email addresses has been lost. The memory stick is encrypted.<br><br>**NB 8. Reporting a 'material' Personal Data Breach to the Data Subject - examples**<br>An example of a reportable Personal Data Breach – An unprotected spreadsheet containing a number of Client's credit card details has left on public transport. The Client's will need to cancel their cards as soon as possible<br>An example of a non-reportable Personal Data Breach – a database containing Client's historical invoicing has become corrupt. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.3.5.3**, **8.3.5.4**, **8.3.5.5**, **8.3.5.9**, **8.3.5.10 and 8.3.5.11** do not apply to Data Processors.<br><br>**8.3.5.12** A Data Processor SHALL report a Personal Data Breach to the Data Controller without undue |

| | |
|---|---|
| | delay and at a minimum within the time period stated in a Data Processing agreement or other contract terms agreed with the Controller.<br>**8.3.5.13** A Data Processor SHALL assist a Data Controller in complying with its own Personal Data Breach reporting obligations. |
| **UK GDPR REFERENCE** | Articles 33 - 34 |
| **AUDIT REFERENCE** | LOCS:23:A21 – Personal Data Breach Management |

### 8.3.6 Data Subject Rights Management

| **CONTROL REFERENCE** | **LOCS:23:C22 – Data Subject Rights Management** |
|---|---|
| **CONTROL OBJECTIVE** | To ensure that any Data Subject request to invoke a right is managed. |
| **CONTROL** | **8.3.6.1** An Organisation SHALL have a defined and internally published Data Subject Rights Request Process.<br>**8.3.6.2** The Organisation SHALL maintain a team or person/s responsible for managing Data Subject requests and SHALL ensure that these staff receive training and resources necessary to respond to requests.<br>**8.3.6.3** The Organisation SHALL provide a self-service mechanism for Data Subjects to exercise their data protection rights.<br>**8.3.6.4** The mechanism SHALL enable the Data Subject to submit a request electronically, verbally or in writing.<br>**8.3.6.5** An Organisation SHALL make all employees aware of the Data Subject Rights Request Process.<br>**8.3.6.6** An Organisation SHALL follow all requirements for a request as laid out in **8.2.1.**<br>**8.3.6.7** When providing a Data Subject's Personal Data in response to a request, the Organisation SHALL do so securely, preferably using links to a secure location or if that is unavailable, password protecting the information.<br>**8.3.6.8** An Organisation SHALL maintain a register of all Data Subject Rights Requests.<br>**8.3.6.9** The Register SHALL record the following information for Data Subject Rights Requests:<br>a. Date of request<br>b. Type of request<br>c. Name<br>d. Contact details<br>e. Data requested<br>f. Identity confirmed (where necessary)<br>g. Actions taken<br>h. Date concluded<br>**8.3.6.10** The Organisation SHALL document an ID verification process indicating the circumstances in which it is necessary to use ID for verification and the types of ID regarded as acceptable.<br>**8.3.6.11** If an extension to respond is needed the Organisation SHALL document the reasons why and update Data Subjects as per **8.2.1.**<br>**8.3.6.12** If a request is refused an Organisation SHALL document the reasons why and inform Data Subjects |

| | |
|---|---|
| | about the reasons for any refusals or exemptions as per **8.2.1**.<br>**8.3.6.13** The staff responsible for managing requests SHOULD meet regularly to discuss any issues and investigate, prioritise or escalate any delayed cases**.** |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** There are a number of rights afforded to Data Subjects. The detail as to the specifics of the right, required responses and any exceptions are listed in **8.2** Data Subject Rights.<br><br>**NB 2.** It is important that all staff are made aware of the process to meet a Data Subject request. An Organisation can maintain a team or person/s to meet Data Subject requests, although it is recommended that the DPO (or equivalent) be involved or oversee the team or person/s. Data Protection training should cover the rights management process including how to recognise a request and what to do.<br><br>**NB 3. The following is an example of a Data Subject Response Process**<br>a. Any requests received by staff to be forwarded to the Data Protection Officer.<br>b. DPO to log request in Data Subject Right Request Register and confirm identity of requestor.<br>c. DPO to respond to requestor confirming the response to the request is underway.<br>d. DPO to consider whether the request should be processed in light of any exemptions.<br>e. DPO to instruct IT with search criteria including systems, time periods and search terms.<br>f. IT to provide results to DPO<br>g. DPO to redact other non-requestor Personal Data.<br>h. If particularly sensitive DPO may submit his decision for approval by the Privacy Council.<br>i. DPO to log the decision of Privacy Council in the Register.<br>j. DPO is to share information with the requestor using secure method (e.g., encrypted memory stick or passworded zip file).<br>**k.** If the original request is denied, the DPO is to inform the requestor of the denial and the reason for the denial. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.3.6.1 – 8.3.6.13** do not apply to Data Processors.<br>**8.3.6.14** If a Data Processor is contacted by a Data Subject regarding any of the Data Subject rights it SHALL contact the Data Controller immediately with details of the request.<br>**8.3.6.15** The Data Processor SHALL assist the Data Controller with meeting its obligation to comply with those rights. |
| **UK GDPR REFERENCE** | Articles 15-22 |
| **AUDIT REFERENCE** | LOCS:23:A22 – Data Subject Rights Management |

### 8.3.7 Technical Security Measures

Technical security measures help protect the Client File data from unapproved access and inadvertent sharing with the wrong parties.

| CONTROL REFERENCE | LOCS:23:C23 – Technical Security Measures |
|---|---|
| **CONTROL OBJECTIVE** | To provide technical security measures for protecting Client File data. |
| **CONTROL** | **8.3.7.1** An Organisation SHALL document the core business systems processing in a systems map, clearly identifying those that process Client File data.: |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** The systems Map can be a very useful tool to assist the DPO with understanding how Client data flows within the Organisation. It could be a graphical representation and should include the following:<br>a. how the systems interact<br>b. data flow<br>c. type of data present<br>d. system owner<br>e. on/off premises<br>f. Access control |
| **CONTROL** | **8.3.7.2** An Organisation SHALL have a documented procedure for applying patches and updates to systems that process Client File data.<br>**8.3.7.3** An Organisation SHALL apply security patches immediately when they become available.<br>**8.3.7.4** An Organisation SHALL apply other non-security related patches regularly and not less than one month after release. |
| **CONTROL APPLICATION GUIDANCE** | **NB 2.** All IT systems that host or process Client File data will from time to time have software patches issued. The Organisation should have an implementation plan that takes into account the seriousness of any vulnerabilities addresses by patches provided. It is recommended that non-security patches are first tried on a test system before being applied to the live Client File.<br><br>**NB 3.** Current and valid certification to ISO 27001/Cyber Essentials may be accepted as supporting evidence of compliance with **8.3.7.2 – 8.3.7.4** in certain circumstances. |
| **CONTROL** | **8.3.7.5** An Organisation SHALL have a backup and restore process in place for all Client data.<br>**8.3.7.6** An Organisation SHALL encrypt at rest all backup data.<br>**8.3.7.7** An Organisation SHALL test the restore function at least weekly.<br>**8.3.7.8** An Organisation SHALL document how the backup and restore function meets criteria laid out in the Business Continuity Plan **(8.1.6).** |
| **CONTROL APPLICATION GUIDANCE** | **NB 4.** It is recommended that a) Recovery Points and b) Recovery Times are agreed with the business and documented in the Business Continuity Plan **(8.1.6).**<br><br>**NB 5.** **8.3.7.7 –** An example of testing the restore function is to delete a test document, recover it from back up and then open to confirm integrity (this may be carried out by IT) |

| | |
|---|---|
| | **NB 6.** Current and valid certification to ISO 27001/Cyber Essentials may be accepted as supporting evidence of compliance with **8.3.7.5 – 8.3.7.8** in certain circumstances. |
| **CONTROL** | **8.3.7.9** An Organisation SHALL have a policy in place governing the use of encryption, including approach to encryption at rest and in transit. The policy SHALL include the requirement for staff training as to the appropriate use of encryption for Client File Data at rest and in transit.<br>**8.3.7.10** At a minimum, encryption SHALL be to NIST Advanced Encryption Standard<br>**8.3.7.11** An Organisation SHALL enable the encryption of data on removable devices that process Client File data.<br>**8.3.7.12** An Organisation SHALL ensure there are processes in place to ensure accuracy, consistency, and completeness of data over the lifecycle of the processing. |
| **CONTROL APPLICATION GUIDANCE** | **NB 7.** Removable devices are at a higher risk of being lost or stolen and therefore need encrypting. This may include (but not limited to), laptops, memory sticks and external drives.<br><br>**NB 8**. Link to NIST AES in normative references above.<br><br>**NB 9.** An example of testing the integrity of data is to carry out a test restore as in **8.3.7.7** or to periodically check with the Client as to data accuracy (**8.1.4.6**) |
| **CONTROL** | **8.3.7.13** An Organisation SHALL protect the network hosting the Client File. |
| **CONTROL APPLICATION GUIDANCE** | **NB 10.** Good network security helps prevent unwanted external access and reduces risks such as data theft and ransomware attacks. Examples of protective technologies include:<br>a. Firewalls<br>b. Anti-Virus/Malware<br>c. Network Access Security<br>d. Penetration Tests<br>e. Multi Factor Authentication<br><br>**NB 11.** Current and valid certification to ISO 27001/Cyber Essentials may be accepted as supporting evidence of compliance with **8.3.7.13** in certain circumstances. |
| **CONTROL** | **8.3.7.14** An Organisation SHALL implement an external vulnerability scan at least once a year.<br>**8.3.7.15** An Organisation SHALL implement an internal vulnerability scan at least once a year. |
| **CONTROL APPLICATION GUIDANCE** | **NB 12.** An external vulnerability scan carried out by a third party will indicate any potential risks such as open port exposures on the Organisation's firewalls.<br><br>**NB 13.** An internal scan will expose any risks present on the internal network.<br><br>**NB 14.** Current and valid certification to ISO 27001/Cyber Essentials may be accepted as supporting evidence of compliance with **8.3.7.14 – 8.3.7.5** in certain circumstances. |

| | |
|---|---|
| **CONTROL** | **8.3.7.16** An Organisation SHALL protect its technology environment by implementing measures that reduce risk of human error. |
| **CONTROL APPLICATION GUIDANCE** | **NB 15.** The biggest risk to breach of Client File data is human error. Solutions that can help reduce the risk of accidental disclosure include:<br>a. Data Leakage Protection<br>b. Threat Detection<br>c. Mobile Device Management<br>d. Training |
| **CONTROL** | **8.3.7.17** An Organisation SHALL use anonymisation, where possible, to reduce the amount of personal data being processed.<br>**8.3.7.18** Where applicable, an Organisation SHALL implement pseudonymisation (see **NB 15**.) as soon as possible when processing Client File personal data, to reduce the risks to the Data Subject. |
| **CONTROL APPLICATION GUIDANCE** | **NB 16.** Pseudonymisation refers to techniques that replace, remove or transform information that identifies an individual. A Data Subject's name can be replaced with a pseudonym, such as a reference number, so that the result can no longer be attributed to that individual, without the use of additional information.<br>**NB 17.** Pseudonymisation can help reduce the risk to the Data Subject concerned but it is still classed as personal data and the Organisation's obligations under UK GDPR and the Data Protection Act 2018 remain.<br>**NB 18**. An example use of anonymisation would be to provide third parties (such as the legal press) with statistical data as to their client demographic without any reference to the Client's identity and in a way that cannot be re-identified.<br>**NB 19**. Applying **8.3.7.17** and/or **8.3.7.18** will assist with compliance with the data minimisation principle (**8.1.4.5**)<br>**NB 20**. ICO guidance on security can be found here |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.3.7** Applies equally to Data Processors. |
| **UK GDPR REFERENCE** | Article 5 (f) Article 32 |
| **AUDIT REFERENCE** | LOCS:23:A23– Technical Security Measures |

### 8.3.8 Organisational Security Measures

| CONTROL REFERENCE | LOCS:23:C24 – Organisational Security Measures |
|---|---|
| **CONTROL OBJECTIVE** | To provide Organisational security measures for protecting Client File data. |
| **CONTROL** | **8.3.8.1** An Organisation SHALL apply role-based access to systems that process Client File data. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** Role based access should take into account where it is necessary for individual actors such as lawyers, legal staff and administrators to access Client data and restrict access where operationally possible. It is recommended that 'Open' systems are avoided (see also **8.3.1.11**). |

| | |
|---|---|
| | **NB 2.** Current and valid certification to ISO 27001/Cyber Essentials may be accepted as supporting evidence of compliance with **8.3.8.1** in certain circumstances. |
| **CONTROL** | **8.3.8.2** An Organisation SHALL keep a record of all its technology assets that process Client File data. |
| **CONTROL APPLICATION GUIDANCE** | **NB 3**. Organisations should record the following details regarding the Assets that process Client File data:<br>a. Device Name<br>b. Device Type<br>c. Serial No<br>d. MAC address<br>e. Primary Device User<br>**NB 4.** Current and valid certification to ISO 27001/Cyber Essentials may be accepted as supporting evidence of compliance with **8.3.8.2** in certain circumstances. |
| **CONTROL** | **8.3.8.3** An Organisation SHALL have a documented electronic equipment disposal process which SHALL include a specification for media sanitisation. |
| **CONTROL APPLICATION GUIDANCE** | **NB 5.** When Personal Data on the Client File has reached the end of its retention period it should be disposed of securely. For electronic data, a good example of this is the NIST 800-88 guidance or IEEE 2883:2022 . It is recommended that IT confirm the disposal.<br><br>**NB 6.** See also the ICO approved certification scheme for asset recovery and destruction here |
| **CONTROL** | **8.3.8.4** An Organisation SHALL dispose of Client File paper documents and files by shredder or confidential waste in line with parameters stated in the Retention & Destruction Policy as laid out in **8.1.7.**<br>**8.3.8.5** When using a third-party service, an Organisation SHALL obtain a certificate of disposal. |
| **CONTROL APPLICATION GUIDANCE** | **NB 7.** Hard Copy data – Paper records should be securely disposed of using a confidential waste facility. |
| **CONTROL** | **8.3.8.6** An Organisation SHOULD implement a clear desk policy.<br>**8.3.8.7** To help prevent unauthorised access to Client Personal Data Organisations SHALL require that all hard copy Client File data be locked away in filing facilities at the end of each working day. |
| **CONTROL APPLICATION GUIDANCE** | **NB 8.** It is recommended that spot checks are carried out to confirm compliance.<br><br>**NB 9.** Current and valid certification to ISO 27001/Cyber Essentials may be accepted as supporting evidence of compliance with **8.3.8.6 – 8.3.8.7** in certain circumstances. |
| **CONTROL** | **8.3.8.8** An Organisation SHALL protect paper documents and files. |
| **CONTROL APPLICATION GUIDANCE** | **NB 10.** When providing physical security to Client File locations which may include offices, meeting rooms, filing cabinets and any IT areas, it is recommended the following are implemented: |

| | |
|---|---|
| | a. Secured Access<br>**b.** Logged access (where possible) |
| **CONTROL** | **8.3.8.9** Where it is necessary to remove Client File data from an Organisation's premises, the Organisation SHALL document best practice guidance for the protection and return of that data.<br>**8.3.8.10** An Organisation SHALL log Client File data leaving and returning to site.<br>**8.3.8.11** An Organisation SHALL implement an authorisation process for removing Client File data from site. |
| **CONTROL APPLICATION GUIDANCE** | **NB 11.** There may be a need to remove Client data in electronic or hard copy from the office for Client visits, court appearances or to work on from home. It is important to have clear policies and best practice guidance as to the treatment of this data.<br>a. Best practice guidance may include:<br>b. Not leaving Client File data unattended<br>c. Reading Client File data in public<br>d. Printing Client File data at home<br>e. Returning Client File data to the office<br>f. Secure disposal of Client File data |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.3.8** applies equally to Data Processors. |
| **UK GDPR REFERENCE** | Article 5 (f) Article 32 |
| **AUDIT REFERENCE** | LOCS:23:A24 – Organisational Security Measures |

### 8.3.9 Data Protection Training

| **CONTROL REFERENCE** | **LOCS:23:C25 – Training** |
|---|---|
| **CONTROL OBJECTIVE** | To ensure continued protection of the Client File through training as to data protection best practice. |
| **CONTROL** | **8.3.9.1** An Organisation SHALL have a documented Data Protection Training Programme for all employees, contractors or others that process data in the Client File.<br>**8.3.9.2** The Data Protection Training where electronic SHALL include a knowledge test with a minimum of 80% pass mark.<br>**8.3.9.3** The Data Protection Training Programme SHALL include an auditable record of training delivered and attended.<br>**8.3.9.4** The Organisation SHALL keep training records which SHALL be monitored to ensure all staff receive and complete Data Protection training.<br>**8.3.9.5** The Data Protection training SHALL be delivered as part of an employee's onboarding process before access to the Client File is granted.<br>**8.3.9.6** The Data Protection training SHALL be delivered at regular intervals (at least annually).<br>**8.3.9.7** A training needs analysis SHALL be conducted and data protection training modules SHALL be modified to meet role specific (front-line) requirements.<br>**8.3.9.8** An Organisation SHALL assign responsibility for managing data protection training. |

| | |
|---|---|
| | **8.3.9.9** An Organisation SHALL provide (internal or external) dedicated and trained resources available to deliver training to all staff,<br>**8.3.9.10** An Organisation SHALL ensure that the training programme is regularly reviewed and signed off by senior management. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** It is recommended that the Data Protection training programme is delivered using multiple channels (presentations, e-learnings, posters, communications etc) and delivered as a series of events over a calendar year.<br>It is recommended that the Data Protection training covers at least the following:<br>a. Definition of Personal Data<br>b. Core areas of Client data Processing<br>c. Sharing Client data with others<br>d. What to do when there is a Personal Data Breach<br>e. What to do when I receive a rights request from a Client<br>f. Working Remotely<br>g. Disposing of Client data<br>h. The importance of providing privacy information to Data Subjects and when to do so.<br>i. Specific modules for front-line staff<br>**NB 2.** **8.3.9.1** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13** |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None - **8.3.9** applies equally to Data Processors. |
| **UK GDPR REFERENCE** | Article 5 (2), Article 39 |
| **AUDIT REFERENCE** | LOCS:23:A25 – Training |

## 8.4 THIRD PARTY SERVICE PROVIDERS AND DATA SHARING

Many Organisations will rely on Third Party vendors or services to assist with the Processing of Client File data. It is important that any protections and safeguards afforded by an Organisation are also provided to an equivalent level (or better) by any Third Parties engaged to assist with the processing of Client file data.

It may also be necessary to share Client File data with Third Parties. That data sharing may also cross borders in which case additional safeguards may be necessary.

### 8.4.1 3rd Party Supplier Register

| CONTROL REFERENCE | LOCS:23:C26 - Supplier Register |
|---|---|
| **CONTROL OBJECTIVE** | To document all Third Parties that supply services relating to the processing of Client File data. |
| **CONTROL** | **8.4.1.1** The Organisation SHALL document all Third Party suppliers that process Client File Personal Data.<br>**8.4.1.2** The Organisation SHALL maintain these records. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** These must be recorded in a Supplier Register.<br>It may be useful to link these back to the ROPA.<br>Suppliers may include (but are not limited to):<br>a. Data Hosting<br>b. External Legal Services<br>c. Barristers<br>d. Translation services<br>e. Transcription services<br>f. Financial Services<br>g. Off-site paper file storage<br>**NB 2.** **8.4.1.1** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13** |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.4.1** equally applies to Data Processors.<br>**NB 3**. See also **8.4.4.3** and **8.4.4.4.** |
| **UK GDPR REFERENCE** | Article 5 (2) |
| **AUDIT REFERENCE** | LOCS:23:A26 - Supplier Register |

### 8.4.2 Supplier Status Assessment

| CONTROL REFERENCE | LOCS:23:C27 – Supplier Status |
|---|---|
| **CONTROL OBJECTIVE** | To determine whether a Third Party service provider is a Data Controller, Joint Controller or a Data Processor. |
| **CONTROL** | **8.4.2.1** An Organisation SHALL determine and document whether a Third Party service provider is a Data Controller, Joint Controller or a Data Processor in relation to processing Client File data.<br>**8.4.2.2** The Organisation, and any Third Party (controller or processor) and, where applicable, their representatives, SHALL cooperate with the Information Commissioner on request.<br>**8.4.2.3** Where it is determined that the Organisation and Third Party are Joint Controllers they SHALL document their respective responsibilities, in particular as regards the exercising of Data Subject rights and their respective |

| | |
|---|---|
| | duties to provide information to the Client, including any relevant contact point. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1. The Data Controller**<br>'Data Controller' means 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. Some controllers may be defined as such under a statutory obligation to process personal data even where they have not determined purpose and means. Section 6(2) of the Data Protection Act 2018 says that anyone who is under such an obligation and only processes data to comply with it will be a controller.<br>For example, a Data Controller will determine:<br>a. how to collect the Personal Data in the first place and the legal basis for doing so;<br>b. which items of Personal Data to collect, i.e. the content of the data;<br>c. the purpose or purposes for which the data are to be used;<br>d. which individuals to collect data about;<br>e. whether to disclose the data, and if so, to whom;<br>f. whether subject access and other individuals' rights apply i.e. the application of exemptions; and<br>g. how long to retain the data or whether to make non-routine amendments to the data.<br><br>**NB 2. The Data Processor**<br>'Data Processor' means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.<br>For example, a Data Processor can determine:<br>a. what information technology (IT) systems or other methods to use to collect Personal Data;<br>b. how to store the Personal Data;<br>c. the detail of the security surrounding the Personal Data;<br>d. the means used to transfer the Personal Data from one Organisation to another;<br>e. the means used to retrieve Personal Data about certain individuals;<br>f. the method for ensuring adherence to a retention schedule;<br>g. the means used to delete or dispose of the data.<br><br>**NB 3. The Joint Controller**<br>Joint Controllers jointly determine the purposes and means of processing the same personal data and consequently share the responsibilities for that data in an agreed, documented, proportionate and relevant manner. Where Controllers have different purposes for Processing the Personal Data they will be independent and not Joint Controllers.<br><br>**NB 4. Examples**<br>An example of a Third Party Data Controller could be a Barrister instructed by a law-firm but who independently determines the purpose and means of the data they will process. |

| | |
|---|---|
| | An example of a Third Party Data Processor is a software as a service (SaaS) hosting platform such as MS Office 365 who process data 'on behalf of' the Organisation.<br>An example of a Joint Controller is where two legal service providers jointly determine the purpose and means of processing the Client's data, share the same purpose of servicing a Client's matter and agree to share the data protection obligations.<br><br>**NB 5.** More detailed guidance on determining whether an Organisation is a controller/processor/joint controller can be found here:<br>https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/ |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.4.2.1-2** applies equally to Data Processors. **8.4.2.3** does not apply.<br><br>**NB 6**. See **NB 2**. for Data Processor definition. See also **8.4.4.3** and **8.4.4.4.** |
| **UK GDPR REFERENCE** | Article 24, Article 26, Article 28, Article 29, Article 31 |
| **AUDIT REFERENCE** | LOCS:23:A27 – Supplier Status |

### 8.4.3 Supplier Risk Assessment

| **CONTROL REFERENCE** | **LOCS:23:C28 – Supplier Risk Assessment** |
|---|---|
| **CONTROL OBJECTIVE** | To determine whether a Third Party Data Processor provides required data protection. |
| **CONTROL** | **8.4.3.1** The Organisation SHALL assess the data protection applied by any Third Party Data Processor that will be processing Client File data to ensure that an equivalent level of data protection is maintained.<br>**8.4.3.2** The Organisation SHALL include the following in a documented due diligence check as a minimum:<br><br>a. Where does Processing take place?<br>b. Do they have a DPO (or equivalent Data Protection lead)?<br>c. Do they have a Breach Reporting Process?<br>d. What technical and Organisational measures are deployed?<br>e. Where (in terms of geography) backup and development data will be located.<br>f. Any relevant Technical & Organisational security measures in place.<br>g. Do standard contract terms include data protection provisions?<br>h. Do they maintain Data Processing Records?<br>i. Will Personal Data be deleted or returned upon termination of contract at no extra cost?<br>j. Do they offer full transparency of data transfer to other parties/destinations?<br>k. Do they have a documented Sub-processor change request process? (i.e. you must have our express permission to effect a change) |

| | |
|---|---|
| | l. Are all agreed data protection provisions included in any sub processor agreements?<br>m. What is the Data Processor's data protection risk assessment process?<br>**8.4.3.3** The Organisation's DPO or equivalent SHALL evaluate the Third Party suppliers answers to determine whether an equivalent level of data protection would be maintained when data is shared.<br>**8.4.3.4** An Organisation SHALL conduct periodic audits of those Data Processors as provided for in the contract at **8.4.4.2 (i).** |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** A good way to achieve this is to create a check list that can be sent to potential Third Party Data Processors. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.4.3** applies equally to Data Processors when engaging sub-processors.<br>**NB 2**. See also **8.4.4.3** and **8.4.4.4.** |
| **UK GDPR REFERENCE** | N/A |
| **AUDIT REFERENCE** | LOCS:23:A28 – Supplier Risk Assessment |

### 8.4.4 Controller to Processor and Processor to Processor Relationships

Whenever a Legal Services Provider uses a Data Processor to process Client File Personal Data on their behalf, a written contract needs to be in place between the parties (C-P).

Similarly, if a Data Processor uses another Organisation (ie a sub-processor) to help it process Personal Data for a Legal Service Provider, it needs to have a written contract in place with that sub-processor (P-P).

Contracts between Legal Service Providers and Data Processors ensure they both understand their obligations, responsibilities and liabilities. Contracts also help them comply with the UK GDPR, and assist Legal Service Providers in demonstrating to Clients and regulators their compliance as required by the accountability principle.

| **CONTROL REFERENCE** | **LOCS:23:C29 – C-P and P-P Data Sharing** |
|---|---|
| **CONTROL OBJECTIVE** | To outline the Organisations requirements for Client File data protection in a Data Processing Agreement. |
| **CONTROL** | **Controller to Processor (C-P)**<br>**8.4.4.1** Where a Data Processor is being engaged, a Data Processing Agreement (DPA) SHALL be agreed by both parties.<br>**8.4.4.2** The Data Processing Agreement SHALL include clauses to ensure the Third Party:<br>a. processes the Personal Data only on documented instructions from the controller, including with regard to transfers of Personal Data to a third country or an international Organisation, unless required to do so by domestic law; in such a case, the processor shall inform the controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;<br>b. ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under a statutory obligation of confidentiality; |

| | |
|---|---|
| | c. takes all measures required to keep information secure;<br>d. does not engage with another processor without prior specific or general written authorisation of the controller;<br>e. ensures that where a processor engages a second processor for carrying out Processing activities on behalf of the controller, the same data protection obligations as set out in the contract between the controller and processor shall be imposed upon the second processor. Where the second processor fails to fulfil its obligations, the first processor remains fully liable;<br>f. assists the controller in responding to requests from individuals to exercise their rights where applicable;<br>g. assists the controller in ensuring compliance with their obligations as concerns keeping information secure, communication of Personal Data Breaches to the Information Commissioner and the Data Subject, and carrying out data protection impact assessments, taking into account the nature of Processing and the information available to the processor;<br>h. at the choice of the controller, deletes or returns all the Personal Data to the controller after the end of the provision of services relating to Processing, and deletes existing copies unless domestic law requires storage of the Personal Data;<br>i. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in **8.4.4** and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller;<br>j. maintain a Record of Processing Activities as laid out in **8.3.3.5.**<br>k. report Personal Data Breaches to the Controller within 24 hours of being made aware. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1**. It may be the case that the contract for services with the Third Party already has sufficient data protection clauses in which case a separate DPA is not needed.<br>**NB 2.** The Data Processor seeking certification may not be working for a controller who is certified to this scheme. |
| **UK GDPR REFERENCE** | Article 28 Article 29 |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **Processor to Processor (P-P)**<br>**8.4.4.3** A Data Processor SHALL gain prior specific or general written authorisation from the Data Controller before engaging another Data Processor as a sub-processor<br>**8.4.4.4** In the case of general written authorisation, the Data Processor SHALL inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Data Controller the opportunity to object to such changes.<br>**8.4.4.5** Where authorisation has been granted, the Data Processor SHALL implement a data processing agreement with the sub-processor. This agreement SHALL contain terms that offer an equivalent level of protection for the personal data as those in the |

| | |
|---|---|
| | contract between the Data Processor and the controller.<br>**8.4.4.6** The Data Processor SHALL require the Sub-Processor to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of UK GDPR.<br>**8.4.4.7** A Data Processor engaging another Data Processor SHALL carry out appropriate due diligence checks (see **8.4.3.2**). |
| **AUDIT REFERENCE** | LOCS:23:A29 – C-P Relationships |

### 8.4.5 Controller to Controller Data Sharing Relationships

Whenever a Legal Services Provider shares Client File data with another Legal Services Provider with Data Controller status or another Controller, a written contract needs to be in place between the parties.

| **CONTROL REFERENCE** | **LOCS:23:C30 – C-C Data Sharing** |
|---|---|
| **CONTROL OBJECTIVE** | To outline the Organisations requirements for Client File data protection in a Data Sharing Agreement. |
| **CONTROL** | **8.4.5.1** Where another Data Controller is being engaged on a routine basis, a Data Sharing Agreement SHALL be agreed and documented by both parties.<br>**8.4.5.2** The Data Sharing Agreement SHALL include:<br>a. The identity of the Data Controllers;<br>b. The purpose of data sharing, including specific aims and why the data sharing is necessary;<br>c. All Organisations involved in the data sharing, including contact details for key personnel and the DPO (or alternative);<br>d. Which data items will be shared;<br>e. The lawful basis for sharing data;<br>f. Relevant conditions for Processing if the data being shared contains Special Category Data or criminal offence data.<br>**8.4.5.3** Where there is a high risk to the Client's rights and freedoms, the Organisation SHALL conduct a DPIA before deciding to share data.<br>**8.4.5.4** The Organisation SHALL log what data is shared, with whom it is shared, and the lawful basis for the data sharing.<br>**8.4.5.5** Where another Data Controller is being engaged on a one-off basis, the Organisation SHALL assess the risk of sharing data, document the Personal Data shared, with whom it is shared, and the lawful basis for sharing. In an urgent or emergency situation, the Organisation SHALL ensure the sharing is necessary and proportionate. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** It is recommended the agreement set out procedures for compliance with individual rights. All Controllers remain responsible for compliance, even if processes set out that separate Controllers carry out particular tasks.<br><br>**NB 2.** It is recommended that a DPIA is carried out even if there is not a high risk to a Client's rights and freedoms, to |

| | |
|---|---|
| | assist in meeting principles of fair and transparent data sharing.<br><br>**NB 3.** **8.4.5.1** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13**<br><br>**NB 4.** More advice on data sharing here https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/ |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.4.5** does not apply to Data Processors. |
| **UK GDPR REFERENCE** | Article 5 (2) and Article 26 |
| **AUDIT REFERENCE** | LOCS:23:A30 – C-C Data Sharing |

### 8.4.6 Transfer of Personal Data outside of the UK

The UK GDPR restricts transfers of Personal Data outside the UK, or the protection of the UK GDPR, unless the rights of the individuals in respect of their Personal Data is protected in another way, or one of a limited number of exceptions applies.

This means that if it is necessary to process Client File Personal Data outside of the UK, and the organisation in the third country is not covered by adequacy regulations, then safeguards must be identified and documented before the transfer can take place. There are a number of options available and the appropriate option should be selected based on the type of data, type of Processing, importing nation's local laws and overall risk to the Client.

If it is necessary to export Client File data a Transfer Risk Assessment (TRA) should be carried out that will determine the level of risk and any associated supplemental protection measures required.

Ultimately the objective is to ensure at least equivalent protection of the Clients data and rights.

| **CONTROL REFERENCE** | **LOCS:23:C31 – Cross Border Data Transfer** |
|---|---|
| **CONTROL OBJECTIVE** | To outline the Organisations requirements for Client File data protection when sharing across borders. |
| **CONTROL** | **8.4.6.1** An Organisation SHALL determine whether the importing Organisation is covered by adequacy regulations. Where that is the case the transfer can take place with no further action.<br>**8.4.6.2** Where the importing Organisation is not covered by an adequacy decision, an exporting Organisation SHALL carry out a Transfer Risk Assessment (TRA) before making a Restricted Transfer (see definitions).<br>**8.4.6.3** The TRA SHALL comprise of the following:<br>a. Location of Data Importer<br>b. Proposed Lawful Transfer Mechanism (BCR/SCC/Derogation)<br>c. What are the specific circumstances of the restricted transfer?<br>d. What is the level of risk to people in the personal information you are transferring?<br>e. What is a reasonable and proportionate level of investigation, given the overall risk level in the personal information and the nature of your organisation? |

f. Is the transfer significantly increasing the risk for people of a human rights breach in the destination country?
g. Are you satisfied that both you and the Data Subjects the information is about will be able to enforce the Article 46 transfer mechanism against the importer in the UK?
h. If enforcement action outside the UK may be needed: Are you satisfied that you and the Data Subjects the information is about will be able to enforce the Article 46 transfer mechanism in the destination country (or elsewhere)?
i. Do any of the exceptions to the restricted transfer rules apply to the "significant risk data" (see NB 5.)?
j. What Personal Data is being transferred?
k. What is the expected duration of the Processing?
l. What is the purpose of the Processing?
m. How sensitive is it?
n. How much is in the public domain?
o. Where did that Personal Data originate from?
p. What technical measures are used to protect that data?
q. What national laws apply in the importer jurisdiction?
r. How are these national laws exercised in practice?
s. Is there any known history of the nation state requiring access to data from the proposed Third Party supplier?
t. Are Supplemental Measures required for this transfer? (if so indicate those to be used)

**8.4.6.4** If an Organisation intends to transfer Client File data outside of the UK to a country without adequacy, it SHALL use one of the following safeguards':

a. Standard data protection clauses specified in regulations made by the Secretary of State under section 17C of the DPA 2018 and for the time being in force;
b. An International Data Transfer Agreement (IDTA)
c. Binding Corporate Rules ratified by the ICO
d. ICO approved Code of Conduct intended as a transfer mechanism (together with binding and enforceable safeguard commitments)
e. ICO approved Certification Schemes intended as a transfer mechanism (together with binding and enforceable safeguard commitments)

**8.4.6.5** Any such transfer legalised by one of the above measures SHALL be communicated to the Client.

**8.4.6.6** In certain circumstances, an exception to the criteria stated in **8.4.6.3** (known as a derogation) may be used. If one of the following derogations is used it SHALL be documented:

a. the Client has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Client due to the absence of an adequacy decision and safeguards;
b. the transfer is necessary for the performance of a contract between the Client and the Organisation or

| | |
|---|---|
| | the implementation of pre-contractual measures taken at the Client's request (occasional use only);<br>c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Client between the controller and another natural or legal person (occasional use only);<br>d. the transfer is necessary for important reasons of public interest;<br>e. An Organisation needs to make the restricted transfer to establish if you have a legal claim, to make a legal claim or to defend a legal claim; (occasional use only)<br>f. An Organisation needs to make the restricted transfer to protect the vital interests of an individual. He or she must be physically or legally incapable of giving consent.;<br>g. the transfer is made from a register which according to domestic law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by domestic law for consultation are fulfilled in the particular case.<br>h. An Organisation is making a one-off restricted transfer and it is in your compelling legitimate interests. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** UK GDPR adequacy regulations can be found here<br><br>**NB 2.** 'Occasional Use' means that the restricted transfer may happen more than once but not regularly.<br><br>**NB 3.** The legitimate interest exception is only for truly exceptional circumstances and where no other accepted safeguards are available.<br><br>**NB 4.** The ICO have provided a TRA tool here<br><br>**NB 5.** The "significant risk data" is the data you identify in **8.4.6.3 (g)** and **8.4.6.3 (h)** as data which your Article 46 transfer mechanism does not provide all the appropriate safeguards for.<br><br>**NB 6.** ICO guidance on International Data Transfer Agreements can be found here |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.4.6.1 – 8.4.6.6** do not apply to Data Processors unless **8.4.6.7** applies in which case the Data Processor SHALL apply **8.4.6.1** – **8.4.6.6.**<br><br>**8.4.6.7** A Data Processor SHALL gain authorisation from the Data Controller before carrying out an international transfer.<br><br>**NB 7.** See also **8.4.4** |
| **UK GDPR REFERENCE** | Articles 44-47, Article 49 |
| **AUDIT REFERENCE** | LOCS:23:A31 – Cross Border Data Transfer |

### 8.4.7 Legal Service Providers not located in the UK

| CONTROL REFERENCE | LOCS:23:C32 – NON-UK Service Providers |
|---|---|
| **CONTROL OBJECTIVE** | To ensure UK representation for Clients whose data is processed by a non-UK domiciled service provider. |
| **CONTROL** | **8.4.7.1** The Data Controller or the Data Processor not established in the UK and processing Client File data SHALL designate in writing a representative in the United Kingdom. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** A representative is not required if Processing is occasional, does not include, on a large scale, special categories of data or Processing is of Personal Data relating to criminal convictions and offences (as referred to in Art 10), and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the Processing.<br><br>**NB 2.** Where the processor of Client File data does not have a UK office, they must inform the Client and/or Legal Service Provider of their officially designated representative in the UK. The representative may be contacted by the ICO, Client or Legal Service Provider regarding data protection matters relating to the Organisation being represented. |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.4.7** applies equally to Data Processors. |
| **UK GDPR REFERENCE** | Article 27 |
| **AUDIT REFERENCE** | LOCS:23:A32 – NON-UK Service Providers |

## 8.5 MONITOR & REVIEW

This section describes the controls designed to enable certification applicants to demonstrate that they are monitoring the implementation of the LOCS:23 controls through the use of regular audits.

### 8.5.1 Internal Audit Process

| CONTROL REFERENCE | LOCS:23:C33 – Internal Audit Process |
|---|---|
| **CONTROL OBJECTIVE** | To ensure that the Organisation is applying LOCS standards to the Client File. |
| **CONTROL** | **8.5.1.1** An Organisation SHALL document an internal audit review process.<br>**8.5.1.2** The internal audit process SHALL include a Control Audit Schedule.<br>**8.5.1.3** The Audit SHALL include all areas indicated by LOCS:23 Audit References in this LOCS:23 Standard.<br>**8.5.1.4** The Organisation SHALL produce an annual Audit Report.<br>**8.5.1.5** The Audit Report SHALL be reviewed by the Privacy Council and at Management Review meetings.<br>**8.5.1.6** The Audit Report SHALL be presented to an external auditor if certification is sought. |
| **CONTROL APPLICATION GUIDANCE** | **NB 1.** When compiling the Control Audit schedule, the Organisation must refer to the LOCS:23 Standard and set its own parameters for the following:<br>a. Control Audit Frequency<br>b. Control Owner<br>c. Audit Sign Off<br>**NB 2.** The Audit schedule should document review dates for all areas indicated as Audit References. It is recommended that the Organisation set the review dates to reflect the importance of the area under review and its likelihood to change. For example, Policy documents could be set for annual review whereas DPIAs could be reviewed monthly.<br>**NB 3. Example Process**<br>a. Diarise annual audit meetings with key business stakeholders<br>b. Design Internal Review Checklist (see appendix 4)<br>c. Complete Internal Review Checklist<br>d. Complete Review Report<br>e. File Checklist and Report<br>f. Report any outstanding risks to Senor Management.<br>**NB 4.** **8.5.1.1** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13** |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | None – **8.5.1** applies equally to Data Processors. |
| **UK GDPR REFERENCE** | Article 5 (2) |
| **AUDIT REFERENCE** | LOCS:23:A33 – Internal Audit Process |

### 8.5.2 Internal Audit Review

| CONTROL REFERENCE | LOCS:23:C34 – Internal Audit |
|---|---|
| **CONTROL OBJECTIVE** | To ensure that applied data protection measures are in place and effective. |
| **CONTROL** | **8.5.2.1** An Organisation SHALL undertake an annual data protection audit and document their findings and recommendations.<br>**8.5.2.2** An Organisation SHALL update Data Protection Measures where necessary in line with audit findings.<br>**8.5.2.3** An Organisation that is a Data Controller SHALL include the following Audit areas:<br>**a. Accountability**<br>This review area focuses on the core Policies, registers and other documentation that ensure the Organisation remain accountable both internally to Senior Management and externally to Data Subjects, Clients and authorities where required. Key auditable areas are:<br>I. Policies (**8.1**)<br>II. ROPA (**8.3.3**)<br>III. Breach Register (**8.3.5.5**)<br>IV. Data Subject Request Register (**8.3.6.8**)<br>V. 3rd Party Supplier Register (**8.4.1**)<br>VI. Awareness Training (**8.3.9**)<br>**b. Privacy by Design**<br>This review area focuses on ensuring that the Organisation builds in privacy by default to all new systems, services and changes to data Processing. Key auditable areas are:<br>I. DPIA (**8.3.2**)<br>II. Default Privacy (**8.3.1**)<br>**c. Privacy Notices**<br>This review area focuses on the Right to Information and ensuring that existing privacy notices are both adequate and relevant. The key auditable privacy notices are:<br>I. Privacy Notices/Privacy information (**8.2.2**)<br>II. Business Processing Privacy Notice (**8.2.2**)<br>**d. Storage Limitation**<br>This review area focuses on the data minimisation principle. The Organisation should ensure that existing policies and schedules are effective and up to date. The Organisation should carry out periodic spot checks to confirm that each business area is actively meeting the requirements laid out in the key policies and procedures including: |

| | |
|---|---|
| | I. Retention Schedule (**8.1.7.6**)<br>II. Retention Policy (**8.1.7**)<br><br>**e. Data Sharing**<br><br>This review area focuses on the Processing activities that require the Organisation to share data with internal and external entities either in Controller to Processor and Controller to Controller relationships either of which could be in cross border locations that may or may not be deemed adequate by the EU or UK. The Organisation is responsible for documenting all transfers and ensuring that safeguarding measures are applied. Key documentation to be audited are:<br><br>I. Transfer Risk Assessment (TRA) (**8.4.6.1**)<br>II. Procurement Due Diligence (**8.4.3.2**)<br>III. Controller to Controller sharing agreements (**8.4.5**)<br>IV. Controller to Processor sharing agreements (**8.4.4**)<br>V. Processor to Processor sharing agreements (**8.4.4**)<br><br>**f. Security**<br><br>This review area focuses on the technical and organisational measures that the Organisation has in place to help protect Personal Data. Technology is changing rapidly and it is essential that the DPO (or equivalent) is kept up to date with all data security developments. Regular meetings with the senior IT team to understand current and future changes is recommended.<br><br>I. New technology (**8.3.7**)<br>II. Access control rights (**8.3.1**)<br>III. Client data sharing practices (**8.3.7**)<br>IV. Use of memory sticks (**8.3.7**)<br>V. Locking of Filing Cabinets (**8.3.8.7**)<br>VI. Vulnerability Scanning (**8.3.7**) |
| **CONTROL APPLICATION GUIDANCE** | **NB 1**. The internal audit will provide the DPO (or equivalent) and Senior Management metrics as to the effectiveness of data protection activities as well as contribute towards an Organisation's accountability (**8.1.4.13**).<br>**NB 2.** **8.5.2** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13** |
| **DATA PROCESSOR ALTERNATIVE CONTROL** | **8.5.2.4** An Organisation that is a Data Processor SHALL apply **8.2.5.3** except for (c) I, (c) II and (e) III.<br>**8.5.2.5** A Data Processor SHALL audit that all areas are consistent with any contracted agreement with a Data Controller and in particular that **8.2.5.3** (a) III, (a) IV, (b) I and (e) I have capacity to assist a Data Controller. |
| **UK GDPR REFERENCE** | Articles 5 and 24 |
| **AUDIT REFERENCE** | LOCS:23:A34 – Internal Audit Review |

# Appendix 1 – Controls Table

The **LOCS:23** standard includes the following assessed controls:

| CLIENT FILE ACTIVITY | CONTROL CATEGORY | CONTROL | CONTROL NAME | REQUIREMENT LEVEL | RELEVANT UK GDPR ARTICLE |
|---|---|---|---|---|---|
| ORGANISATION GOVERNANCE | GOVERNANCE | LOCS:23:C1 | Privacy Council | **SHALL** | Article 5 |
| ORGANISATION GOVERNANCE | GOVERNANCE | LOCS:23:C2 | DPO decision | **SHALL**<br>**SHOULD** | Article 5<br>Article 37<br>Article 38<br>Article 39 |
| ORGANISATION GOVERNANCE | GOVERNANCE | LOCS:23:C3 | Registration | **SHALL** | Article 5 |
| WORKING ON FILE | GOVERNANCE | LOCS:23:C4 | Principles | **SHALL**<br>**SHOULD** | Article 5 |
| WORKING ON FILE | GOVERNANCE | LOCS:23:C5 | Data Protection and Information Security Policies | **SHALL**<br>**SHOULD** | Article 5 |
| WORKING ON FILE | GOVERNANCE | LOCS:23:C6 | Business Continuity Policy | **SHALL**<br>**SHOULD** | Article 5 |
| CLOSING FILE (ARCHIVING) | GOVERNANCE | LOCS:23:C7 | Data retention & Destruction Policy | **SHALL**<br>**SHOULD** | Article 5 |
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C8 | Transparency & Communication | **SHALL**<br>**SHALL NOT** | Article 11<br>Article 12 |
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C9 | Right to Information | **SHALL** | Article 13<br>Article 14<br>Article 23 |
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C10 | Right to Access | **SHALL**<br>**SHALL NOT** | Article 15<br>Article 23 |
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C11 | Right to Rectification | **SHALL** | Article 16<br>Article 19<br>Article 23 |
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C12 | Right to Erasure | **SHALL**<br>**SHALL NOT** | Article 17<br>Article 19<br>Article 23 |

| | | | | | |
|---|---|---|---|---|---|
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C13 | Right to Restrict Processing | **SHALL**<br>**SHALL NOT** | Article 18<br>Article 19<br>Article 23 |
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C14 | Right to Portability | **SHALL** | Article 20<br>Article 23 |
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C15 | Right to Object | **SHALL** | Article 21<br>Article 23 |
| WORKING ON FILE – CLIENT ENGAGEMENT | DATA SUBJECT RIGHTS | LOCS:23:C16 | Automated Decision Making | **SHALL**<br>**SHALL NOT** | Article 22<br>Article 23 |
| FILE GOVERNANCE | OPERATIONAL PRIVACY | LOCS:23:C17 | Default Privacy | **SHALL** | Article 25 |
| FILE GOVERNANCE | OPERATIONAL PRIVACY | LOCS:23:C18 | DPIA | **SHALL**<br>**SHOULD** | Article 35<br>Article 36 |
| FILE GOVERNANCE | OPERATIONAL PRIVACY | LOCS:23:C19 | ROPA | **SHALL**<br>**SHOULD** | Article 30 |
| WORKING ON FILE | OPERATIONAL PRIVACY | LOCS:23:C20 | Lawful Processing | **SHALL**<br>**SHALL NOT**<br>**SHOULD** | Article 6<br>Article 7<br>Article 9<br>Article 10 |
| WORKING ON FILE – CLIENT ENGAGEMENT | OPERATIONAL PRIVACY | LOCS:23:C21 | Personal Data Breach Management | **SHALL** | Articles 33 – 34 |
| WORKING ON FILE – CLIENT ENGAGEMENT | OPERATIONAL PRIVACY | LOCS:23:C22 | Data Subject Rights Management | **SHALL**<br>**SHOULD** | Articles 15-22 |
| FILE GOVERNANCE | OPERATIONAL PRIVACY | LOCS:23:C23 | Technical Security Measures | **SHALL** | Article 5<br>Article 32 |
| FILE GOVERNANCE | OPERATIONAL PRIVACY | LOCS:23:C24 | Organisational Security Measures | **SHALL**<br>**SHOULD** | Article 5<br>Article 32 |
| ORGANISATION GOVERNANCE | OPERATIONAL PRIVACY | LOCS:23:C25 | Training | **SHALL** | Article 5<br>Article 39 |
| WORKING ON FILE – 3rd PARTIES | THIRD PARTY SERVICE PROVIDERS & DATA SHARING | LOCS:23:C26 | Supplier Register | **SHALL** | Article 5 |
| WORKING ON FILE – 3rd PARTIES | THIRD PARTY SERVICE PROVIDERS & DATA SHARING | LOCS:23:C27 | Supplier Status | **SHALL** | Article 24<br>Article 26<br>Article 28<br>Article 29<br>Article 31 |
| WORKING ON FILE – 3rd PARTIES | THIRD PARTY SERVICE PROVIDERS & DATA SHARING | LOCS:23:C28 | Supplier Risk Assessment | **SHALL** | Article 28 |

| | | | | | |
|---|---|---|---|---|---|
| WORKING ON FILE – 3rd PARTIES | THIRD PARTY SERVICE PROVIDERS & DATA SHARING | LOCS:23:C29 | C-P and P-P Relationships | **SHALL** | Article 28<br>Article 29 |
| WORKING ON FILE – 3rd PARTIES | THIRD PARTY SERVICE PROVIDERS & DATA SHARING | LOCS:23:C30 | C-C Data Sharing | **SHALL** | Article 5<br>Article 26 |
| WORKING ON FILE – 3rd PARTIES | THIRD PARTY SERVICE PROVIDERS & DATA SHARING | LOCS:23:C31 | Cross Border Data Transfer | **SHALL** | Article 44<br>Article 45<br>Article 46<br>Article 47<br>Article 49 |
| WORKING ON FILE – 3rd PARTIES | THIRD PARTY SERVICE PROVIDERS & DATA SHARING | LOCS:23:C32 | Non-UK Service Providers | **SHALL** | Article 27 |
| FILE GOVERNANCE | MONITORING & REVIEW | LOCS:23:C33 | Internal Audit | **SHALL** | Article 5 |
| FILE GOVERNANCE | MONITORING & REVIEW | LOCS:23:C34 | Internal Audit Review | **SHALL** | Article 24 |

# Appendix 2 – UK GDPR Applicability

The following table indicates the applicability of the UK GDPR articles to the LOCS:23 standard

| | | | |
|---|---|---|---|
| Article 1 | N/A | Article 51 | N/A |
| Article 2 | N/A | Article 52 | N/A |
| Article 3 | N/A | Article 53 | N/A |
| Article 4 | Where terms are used which are defined within the UK GDPR the same definition has been adopted and used for the LOCS:23 Standard | Article 54 | N/A |
| Article 5 | LOCS:23:C1<br>LOCS:23:C2<br>LOCS:23:C3<br>LOCS:23:C4<br>LOCS:23:C5<br>LOCS:23:C6<br>LOCS:23:C7<br>LOCS:23:C23<br>LOCS:23:C24<br>LOCS:23:C25<br>LOCS:23:C26<br>LOCS:23:C30<br>LOCS:23:C33<br>LOCS:23:C34 | Article 55 | N/A |
| Article 6 | LOCS:23:C20 | Article 56 | N/A |
| Article 7 | LOCS:23:C20 | Article 57 | N/A |
| Article 8 | N/A | Article 58 | N/A |
| Article 9 | LOCS:23:C20 | Article 59 | N/A |
| Article 10 | LOCS:23:C20 | Article 60 | N/A |
| Article 11 | LOCS:23:C8 | Article 61 | N/A |
| Article 12 | LOCS:23:C8 | Article 62 | N/A |
| Article 13 | LOCS:23:C9 | Article 63 | N/A |
| Article 14 | LOCS:23:C9 | Article 64 | N/A |
| Article 15 | LOCS:23:C10<br>LOCS:23:C22 | Article 65 | N/A |
| Article 16 | LOCS:23:C11<br>LOCS:23:C22 | Article 67 | N/A |

| | | | |
|---|---|---|---|
| Article 17 | LOCS:23:C12<br>LOCS:23:C22 | Article 68 | N/A |
| Article 18 | LOCS:23:C13<br>LOCS:23:C22 | Article 69 | N/A |
| Article 19 | LOCS:23:C11 – C13<br>LOCS:23:C22 | Article 70 | N/A |
| Article 20 | LOCS:23:C14<br>LOCS:23:C22 | Article 71 | N/A |
| Article 21 | LOCS:23:C15<br>LOCS:23:C22 | Article 72 | N/A |
| Article 22 | LOCS:23:C16<br>LOCS:23:C22 | Article 73 | N/A |
| Article 23 | LOCS:23:C8 – C16 | Article 74 | N/A |
| Article 24 | LOCS:23:C34 | Article 75 | N/A |
| Article 25 | LOCS:23:C17 | Article 76 | N/A |
| Article 26 | LOCS:23:C27<br>LOCS:23:C30 | Article 77 | LOCS:23:C8 |
| Article 27 | LOCS:23:C32 | Article 78 | N/A |
| Article 28 | LOCS:23:C27<br>LOCS:23:C29 | Article 79 | LOCS:23:C8 |
| Article 29 | LOCS:23:C27<br>LOCS:23:C29 | Article 80 | N/A |
| Article 30 | LOCS:23:C19 | Article 81 | N/A |
| Article 31 | LOCS:23:C27 | Article 82 | N/A |
| Article 32 | LOCS:23:C23<br>LOCS:23:C24 | Article 83 | N/A |
| Article 33 | LOCS:23:C21 | Article 84 | N/A |
| Article 34 | LOCS:23:C21 | Article 85 | N/A |
| Article 35 | LOCS:23:C18 | Article 86 | N/A |
| Article 36 | LOCS:23:C18 | Article 87 | N/A |
| Article 37 | LOCS:23:C2 | Article 88 | N/A |
| Article 38 | LOCS:23:C2 | Article 89 | N/A |
| Article 39 | LOCS:23:C2<br>LOCS:23:C25 | Article 90 | N/A |
| Article 40 | N/A | Article 91 | N/A |
| Article 41 | N/A | Article 92 | N/A |
| Article 42 | N/A | Article 93 | N/A |
| Article 43 | N/A | Article 94 | N/A |
| Article 44 | LOCS:23:C31 | Article 95 | N/A |

| | | | |
|---|---|---|---|
| Article 45 | LOCS:23:C31 | Article 96 | N/A |
| Article 46 | LOCS:23:C31 | Article 97 | N/A |
| Article 47 | LOCS:23:C31 | Article 98 | N/A |
| Article 48 | N/A | Article 99 | N/A |
| Article 49 | LOCS:23:C31 | | |
| Article 50 | N/A | | |

# Appendix 3 – Data Processor Control Applicability

| CONTROL REFERENCE | NOTES |
|---|---|
| LOCS:23:C1 Privacy Council | does not apply to Data Processors |
| LOCS:23:C2 –DPO | applies to Data Processors |
| LOCS:23:C3 – ICO Registration | applies to Data Processors |
| LOCS:23:C4 – Principles | partially applies to Data Processors |
| LOCS:23:C5 – Data Policy Document | applies to Data Processors |
| LOCS:23:C6– BC Policy Document | applies to Data Processors |
| LOCS:23:C7– R&D Policy Document | does not apply to Data Processors |
| LOCS:23:C8– Transparency & Communication | partially applies to Data Processors |
| LOCS:23:C9 – Right to Information | does not apply to Data Processors (See **8.3.6.14** and **8.3.6.15)** |
| LOCS:23:C10– Right of access | does not apply to Data Processors (See **8.3.6.14** and **8.3.6.15)** |
| LOCS:23:C11– Right of Rectification | does not apply to Data Processors (See **8.3.6.14** and **8.3.6.15)** |
| LOCS:23:C12– Right of Erasure | does not apply to Data Processors (See **8.3.6.14** and **8.3.6.15)** |
| LOCS:23:C13– Right to Restriction of Processing | does not apply to Data Processors (See **8.3.6.14** and **8.3.6.15)** |
| LOCS:23:C14 – Right to Portability | does not apply to Data Processors (See **8.3.6.14** and **8.3.6.15)** |
| LOCS:23:C15 – Right to Object | does not apply to Data Processors (See **8.3.6.14** and **8.3.6.15)** |
| LOCS:23:C16 – Automated Decision Making | does not apply to Data Processors (See **8.3.6.14** and **8.3.6.15)** |
| LOCS:23:C17 – Default Privacy | applies to Data Processors |
| LOCS:23:C18 – DPIA | partially applies to Data Processors |
| LOCS:23:C19 – ROPA | partially applies to Data Processors |
| LOCS:23:C20 – Lawful Processing | does not apply to Data Processors |
| LOCS:23:C21 – Personal Data Breach Management | partially applies to Data Processors |
| LOCS:23:C22 – Data Subject Rights Management | partially applies to Data Processors |
| LOCS:23:C23– Technical Security Measures | applies to Data Processors |
| LOCS:23:C24 – Organisational Security Measures | applies to Data Processors |
| LOCS:23:C25 – Training | applies to Data Processors |
| LOCS:23:C26 - Supplier Register | applies to Data Processors |
| LOCS:23:C27 – Supplier Status | partially applies to Data Processors |

| | |
|---|---|
| LOCS:23:C28 – Supplier Risk Assessment | applies to Data Processors |
| LOCS:23:C29 – C-P and P-P Relationships | partially applies to Data Processors |
| LOCS:23:C30 – C-C Data Sharing | does not apply to Data Processors |
| LOCS:23:C31 – Cross Border Data Transfer | partially applies to Data Processors |
| LOCS:23:C32 – NON-UK Service Providers | applies to Data Processors |
| LOCS:23:C33 – Internal Audit Process | applies to Data Processors |
| LOCS:23:C34 – Internal Audit Review | partially applies to Data Processors |

# Appendix 4 – LOCS:23 Self-Audit Checklist template

Use this template as a checklist to assist with meeting requirements of **8.5.1**.

| AUDIT REFERENCE | COMPLETE Y/N | NOTES |
|---|---|---|
| LOCS:23:A1 Privacy Council | | |
| LOCS:23:A2 –DPO | | |
| LOCS:23:A3 – ICO Registration | | |
| LOCS:23:A4 – Principles | | |
| LOCS:23:A5 – Data Policy Document | | |
| LOCS:23:A6– BC Policy Document | | |
| LOCS:23:A7– R&D Policy Document | | |
| LOCS:23:A8– Transparency & Communication | | |
| LOCS:23:A9 – Right to Information | | |
| LOCS:23:A10– Right of access | | |
| LOCS:23:A11– Right of Rectification | | |
| LOCS:23:A12– Right of Erasure | | |
| LOCS:23:A13– Right to Restriction of Processing | | |
| LOCS:23:A14 – Right to Portability | | |
| LOCS:23:A15 - Right to Object | | |
| LOCS:23:A16 – Automated Decision Making | | |
| LOCS:23:A17 – Default Privacy | | |
| LOCS:23:A18 – DPIA | | |
| LOCS:23:A19 – ROPA | | |
| LOCS:23:A20 – Lawful Processing | | |
| LOCS:23:A21 – Personal Data Breach Management | | |
| LOCS:23:A22 – Data Subject Rights Management | | |
| LOCS:23:A23– Technical Security Measures | | |
| LOCS:23:A24 – Organisational Security Measures | | |
| LOCS:23:A25 – Training | | |

| | | |
|---|---|---|
| LOCS:23:A26 - Supplier Register | | |
| LOCS:23:A27 – Supplier Status | | |
| LOCS:23:A28 – Supplier Risk Assessment | | |
| LOCS:23:A29 – C-P and P-P Relationships | | |
| LOCS:23:A30 – C-C Data Sharing | | |
| LOCS:23:A31 – Cross Border Data Transfer | | |
| LOCS:23:A32 – NON-UK Service Providers | | |
| LOCS:23:A33 – Internal Audit Process | | |
| LOCS:23:A34 – Internal Audit Review | | |