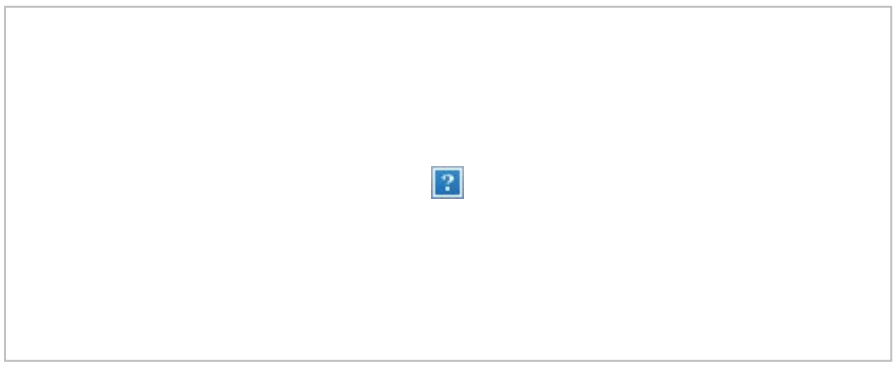
From:	timhyman@2twenty4consulting.com
To:	certification
Subject:	ICO Certification Scheme
Date:	24 August 2021 15:19:43
Attachments:	image001.png gdpr-certification-criteria-approval-submission-form-20210101.docx LOCS Assessment Criteria.docx LOCS Certification Scheme Application.docx LOCS Certification Standard.doc LOCS Control Audit Checklist.xlsx LOCS Control Audit Schedule.xlsx

---

Please find attached the application form and associated documentation

Many thanks

Tim



Please complete the following application form in support of your UK GDPR certification scheme criteria submission and send to certification@ico.org.uk
Please complete the entire form or it may be returned and delay the approval process.

Article 42 UK GDPR Certification Criteria Approval submission form

Our detailed certification guidance sets out the requirements for certification scheme criteria. Please read and ensure that your criteria meet the requirements before submitting them for approval, as these are the requirements on which our assessment will be based.

Please note that as a public authority we are subject to the Freedom of Information Act 2000 (FOIA). We will treat any FOI requests on a case-by-case basis. Therefore, when submitting information to us you should clearly indicate anything that you consider confidential or commercially sensitive.

Date of submission
24/08/21

Details of scheme/ criteria owner	
Company Name (Please provide the full name of your organisation and any relevant trading or legal entity names relevant to this submission)	2twenty4Consulting Ltd
Type of legal entity	Limited Company
Companies house registration number	07755609
ICO registration number (unless exempt)	ZA377863
Physical address	70 Croft Road Hastings TN34 3HE
Telephone number	07500227009
Website address	www.2twenty4consulting.com
Main point of contact (and contact details)	Tim Hyman timhyman@2twenty4consulting.com
Are you a certification body also seeking accreditation or separate entity? (Provide UKAS accreditation details if relevant.)	Yes ☐ No ☒
Scheme criteria details	
Name of data protection scheme/ standard/ criteria	Legal Services Operational Privacy Certification Scheme (LOCS:21)

Submitted version number	1
Are criteria part of a full certification (conformity assessment) scheme?	Yes ☒ No ☐
If 'yes' provide scheme name and include relevant documentation (eg. scheme manual outlining audit methodology)	Scheme Name is LOCS:21 Documents associated with the application are as follows LOCS:21 Application Notes LOCS:21 Standard LOCS:21 Assessment Guide LOCS:21 Audit Checklist LOCS:21 Audit Schedule
Have any potential certification bodies been identified at this stage? (If so provide details)	Yes ☐ No ☒
Scope – briefly describe scope of scheme criteria (please also provide reference to relevant section of documentation)	The overall scope is for the management of the Client Data File and has the following qualification Applicant Scope • Law firms • Solicitors • Actuaries • Other providers of legal services • Suppliers to Legal Service Providers Processing Scope • Collection of client personal data; • Storage of client personal data whether long term or transient; • Modification of client data; • 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;
Are criteria designed to be applied to processing operations that constitute a product or service and therefore are suitable for use under ISO 17065/2012?	Yes ☒ No ☐
Where have you included an explanatory statement covering the background to the development of the scheme criteria?	This is detailed in the document LOCS:21 Application Notes
What is your intended target market? (ie. specific sector/ industry/ product or service that criteria/scheme are aimed at)	The intended market Legal Service Providers which primarily consists of law firms, solicitors and barristers but will include notaries and other specialist legal services. To ensure the entire legal 'supply chain' is covered the standard will also apply to the suppliers used by the Legal Service Providers.

Have you provided evidence of market support for a scheme based on the criteria submitted? (Please also provide reference to relevant section of documentation)	This is detailed in the document LOCS:21 Application Notes
Describe how the criteria are likely to improve data protection compliance of controllers and processors. (Please also provide reference to relevant section of documentation)	In the absence of a certification, current levels of protection vary drastically and are based on individual interpretation. This means the general public have to 'trust' that the Legal Service Providers they select are applying appropriate protection to their personal data. The standard will promote and improve data protection within Legal Service Providers and their supply chain by providing a practical, achievable and certifiable set of controls. The ratification by the ICO will add the gravitas needed that will drive Legal Service Providers to adopt the standard and in turn demonstrate best practice to their clients.
Describe how data subjects will benefit in respect of their information rights, including explaining desired outcomes to data subjects. (Please also provide reference to relevant section of documentation)	Data Subjects on seeing the certification will gain the confidence that the Legal Service Provider has demonstrated it can meet all data subject rights criteria including the access, rectification, erasure and appropriate protection of their data. This is a core requirement in the LOCS:21 standard
Does the criteria catalogue/standard contain all the sections outlined in our detailed certification guidance?	Yes ☒ No ☐
Are all aspects of UK GDPR covered? If anything has been excluded due to scope of criteria please explain which ones and reasons.	All areas are covered
Do the criteria include an explanation (where appropriate) and implementation guidance for controllers/processors?	Yes ☒ No ☐
Where do criteria describe how ToE should be defined by controller or processor?	This is detailed in the document LOCS:21 Standard
Where are relevant terms defined and normative references identified?	This is detailed in the document LOCS:21 Standard
Have you carried out any testing? If so have you provided results?	Yes ☒ No ☐
If not, have you provided a worked example to demonstrate how the criteria might be applied in practice.	Yes ☐ No ☐
Can the criteria catalogue be published as submitted to the ICO? (in line with UK GDPR requirements.)	Yes ☒ No ☐
If not, have you provided a publicy available version?	Yes ☐ No ☐

Documentation	
Please list all documents included in your submission with brief description of contents	
Document name	Description

LOCS:21 Application Notes	This document describes the development of the scheme, the market demand, benefits to data subjects and other ICO requirements
LOCS:21 Standard	This is the set of controls required to meet the LOCS:21 standard
LOCS:21 Assessment Guide	This is the guidance for assessors as to how to audit and award certification where appropriate
LOCS:21 Audit Checklist	This is a template for organiosations to assist with an internal self-audit
LOCS:21 Audit Schedule	This is a template for organisations to assist with the scheduling of an internal audit

LEGAL SERVICES OPERATIONAL PRIVACY CERTIFICATION SCHEME

AUGUST 2021

LOCS:21 ASSESSMENT CRITERIA

2TWENTY4 CONSULTING
DATA PROTECTION SERVICES

Contents

Introduction

This document sets out the criteria, methodology and process for accrediting an applicant organisation with LOCS:21 certification

It is intended that the ICO approve certification bodies who are able to award the LOCS:21 accreditation.

Successful accreditation will require applicant organisations to meet the criteria laid out in this document as it relates to four core areas of audit

1. Governance
2. Operational Privacy
3. Monitoring & Review
4. Continuous Improvement

Within those core areas are listed 31 core controls that define the requirements of the overall standard.

Each control has one or more Control Audit criteria that are used for both internal self-audits and to assess overall compliance for accreditation.

There are 28 Control Audits used for certification.

Compliance requirements

LOCS:21 uses the following compliance requirement terms:

MUST(G)	this is mandatory to achieve the LOCS:21 accreditation and mandatory under UK GDPR.
MUST	this is mandatory to achieve the LOCS:21 accreditation
SHOULD	this is not required to achieve the LOCS:21 accreditation but constitutes current best practice.
OPTION	this describes something that may be applied but is not required to achieve the LOCS:21 accreditation.

Assessment Qualification

1 Applicant Scope

An applicant MUST provide services within one of the following two categories

CATEGORY A – Legal Service Providers

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

CATEGORY B – Legal Service Provider Suppliers

- 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 Processing Scope

The Applicant MUST process data that relates to the Client Data File by providing services that include one of the following activities:

- Collection of client personal data;
- Storage of client personal data whether long term or transient;
- Modification of client data;
- 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;

Assessment Methodology

The assessment is binary in nature and ultimately has two possible outcomes; Pass or Fail.

The assessor will use the following assessment criteria for each control audit:

Compliant	there is satisfactory evidence this control is in place and meets acceptable levels
Partially Met	there is some evidence that this control is in place but further action is required
Not met	there is insufficient evidence that this control is in place

Applicant Organisations must meet 100% compliance of the 15 MUST(G) controls and 100% compliance for 11 out of the other 13 MUST controls to achieve PASS status and certification. Two of the MUST controls may be PARTIALLY MET to achieve PASS status. Any controls NOT MET will result in a FAIL status.

Application Process

1 Applicants submit initial application

2 Assessor determines eligibility and confirms or denies application

3 Applicant submits evidence of compliance for all Control Audits

4 Assessor makes preliminary assessment and requests further evidence if required

5 Applicant submits any further evidence requested

6 Assessor makes final review

7 If the outcome is PASS the applicant will be provided with a certificate and use of LOCS:21 logo

8 If the outcome is FAIL the applicant may request re-assessment following addressing of any partially Met or Not Met control audits.

9 Assessor will re-assess

NOTE: Where a control is only PARTIALLY MET or NOT MET the assessor will advise as to any mitigations or required improvements.

Compliance Criteria

The following are the detailed criteria required for assessing each Control Audit.

CONTROL	NAME	LEVEL	REQUIREMENT
LOCS:21:A1	SCOPE DOCUMENT	MUST	Applicant must provide documented details of the scope for certification which should include: • Geographies within scope • Offices within scope • Systems within scope • Organisational objectives for personal data management
LOCS:21:A2	PRI CON	MUST	Applicant must provide documented Privacy Management organisation structure *NOTE – the assessor must determine the likely effectiveness of the proposal*
LOCS:21:A3	DPO DOCUMENT	MUST (G)	Applicant must provide a documented decision made for Senior Privacy Role *NOTE – the assessor must ensure this decision meets UKGDPR DPO requirements*
LOCS:21:A4	POLICY DOCUMENTS	MUST (G)	Applicant must publish either a single Data Protection Policy containing all required categories or individual policies for each of the following categories. • Data Protection Policy • Acceptable Use Policy • User Account Policy • Removable Device Policy • Service Procurement Policy • Remote Access Policy • Business Continuity Policy

			• Retention Policy • Destruction Policy *NOTE – the assessor must determine whether the policy requirements are adequate taking into account the size and processing activities of the applicant*
LOCS:21:A5	DPIA DOCUMENT	MUST (G)	Applicant must publish a DPIA Template
LOCS:21:A6	ROPA	MUST (G)	Applicant must maintain a Record of Processing Activities
LOCS:21:A7	LAWFUL BASIS	MUST (G)	Applicant must record the lawful basis for processing activities *NOTE – This does not have to be a separate document and can be a line item in the ROPA*
LOCS:21:A8	RISK REGISTER	MUST	Applicant must maintain a risk register based on all identifiable risks including those introduced via the DPIA process. This should include at least: • Type of risk • Level of risk • Priority of risk • Owner of risk • Proposed mitigation
LOCS:21:A9	SUPPLIER REGISTER	MUST	Applicant must maintain a register of all third-party service suppliers where personal data is processed. This must include • Name of processor • Type of processing • Type of data processed • Location of processing
LOCS:21:A10	ADEQUACY CHECKLIST	MUST	Applicant must provide evidence of an adequacy checklist used for third-party service suppliers that have Data Controller status
LOCS:21:A11	DPA	MUST (G)	Applicant must provide evidence of a Data Processing Agreement available for use with third party suppliers where appropriate. *NOTE - This must meet the UK GDPR Art 28 requirements*
LOCS:21:A12	INTTRAN	MUST (G)	Applicant must record the legal mechanism used for cross-border data transfers. This must include the following: • Name of data importer • Location of data importer • Legal mechanism used (adequacy, BCR, SCC, derogation etc) • Any supplemental measures
LOCS:21:A13	PRIVACY NOTICE	MUST (G)	Applicant must have a Privacy Notice that meets the UK GDPR requirement
LOCS:21:A15	BREACH REGISTER	MUST (G)	Applicant must keep a register of all data breach activity. This must include the following

			• The date and time the breach was made known to the organisation • The date and time the breach occurred. • The name of the individual or supplier reporting the breach • The nature of the data breach • The categories and approximate number of data subjects concerned • The categories and approximate number of data records concerned; • Describe the likely consequences of the data breach; • Describe the measures taken or proposed to be taken by the controller to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.
LOCS:21:A16	SAR REGISTER	MUST (G)	Applicant must keep a register of all data subject request activity. This must include the following: • Date of request • Type of request • Name • Contact details • Data requested • Identity confirmed • Actions taken • Date concluded
LOCS:21:A18	PATCH PROCEDURE	MUST	Applicant must document patching schedule for core business applications
LOCS:21:A19	RDP	MUST	Applicant must document protective measures for removable devices that could contain personal data
LOCS:21:A20	GATEWAY PROTECTION	MUST	Applicant must document the protective measures applied at the firms IT infrastructure gateway (e.g. firewalls etc)
LOCS:21:A21	USER ACCESS	MUST	Applicant must apply a strong password requirement
LOCS:21:A23	ACCESS CONTROL	MUST (G)	Applicant must document how role based access is applied to core business systems
LOCS:21:A24	ASSET REGISTER	MUST	Applicant must keep a record all information assets
LOCS:21:A25	SECURE DISPOSAL	MUST	Applicant must maintain secure disposal procedures for paper and electronic records

LOCS:21:A26	DR/BC TEST	MUST	Applicant must maintain a Business Continuity/Disaster Recovery procedure and test schedule
LOCS:21:A27	DS RIGHTS	MUST (G)	Applicant must maintain internal processes for meeting data subject rights
LOCS:21:A28	BREACH REPORTING DOCUMENTATION	MUST (G)	Applicant must maintain breach reporting documentation including Breach Report Form and Breach Handling Process
LOCS:21:A29	SAR DOCUMENTATION	MUST (G)	Applicant must maintain Data Subject Access documentation including SAR Form and internal SAR procedure
LOCS:21:A30	CAS	MUST	Applicant must maintain this Control Audit Schedule NOTE – Initial applications only need to confirm intention to use the Audit Schedule whereas renewals must evidence usage.
LOCS:21:A31	UAP	MUST (G)	Applicant must document a User Awareness Program and maintain an attendance log

Certificate

Assessors must provide a certificate to applicants that pass the LOCS:21 assessment

This certificate must contain the text ‘LOCS:21 CERTIFICATION’ and include

- Date of passing
- Name of Applicant
- LOCs:21 logo

The style of certificate is the choice of the assessor who may also add their own logo

LEGAL SERVICES OPERATIONAL PRIVACY CERTIFICATION SCHEME

AUGUST 2021 | **LOCS:21 APPLICATION NOTES**

2TWENTY4 CONSULTING
DATA PROTECTION SERVICES

Introduction

Having spent 25 years in and around the Legal Service industry, and in particular the IT and Privacy functions, I have a good understanding of the inherent challenges.

It is well known that law firms and other Legal Service Providers (LFPs) process significant amounts of personal data including in many cases sensitive personal data.

The majority of Law firms have taken Information Security and Data Protection very seriously but the ability to demonstrate this both internally and to clients remains a significant challenge.

In 2016 I read the first publication of GDPR and although there were 2 years to prepare for its formal application I could see what the impact would be on LSPs and there support functions.

Later that year I spoke at a conference attended by around 500 Law Firm senior IT professionals and highlighted what would be in my opinion the main practical challenges of GDPR. Following an active Q & A session and many follow up meetings a number of consistent challenges were discussed:

- There was an increasing demand from clients for heightened Information Security
- The only recognised certification was ISO 27001
- ISO 27001 was expensive, time consuming and resource hungry – ruling it out for most small and medium size law firms.
- There was a tendency to view the adoption of a standard as ISO27001 or nothing and therefore if we cannot do ISO 27001 we will do nothing
- There was a false perception that ISO 27001 would ensure future GDPR compliance
- There was a demand for a practical and affordable ISO 27001 alternative

Over the next 2 years I developed a new standard for Information Security and included some key elements of the upcoming GDPR – this was called PROSEC 2.0.

Four law firms adopted PROSEC2 which included a set of information security and data protection standards, a built-in audit scheme and a certification process.

The law firms Charles Russell Speechleys, Stephens & Bolton, Ashfords and Foot Anstey varied in size location and type of law practiced so were a good test for the new standard.

I am now a Data Protection Officer and certified as a DPO at the University of Maastricht. Whilst I fully appreciate that GDPR specifically rules out the certification of individuals from the approved Certification Schemes, I have seen firsthand the significant impact certification has on building and promoting client trust.

The general feedback to this day for the PROSEC2.0 standard is that whilst an affordable and practical standard that supports reflects ISO27001 is very welcome it lacks one key facet – market recognition.

This is why a new Certification Scheme focussed on Data Protection but one that also supports and respects ISO 27001 and one that has the gravitas of the ICO as verification will be the ‘recognised’ accreditation that the industry is desperate for – both to boost client confidence and demonstrate internal governance.

ICO Justification Criteria

any general/sectoral/industry data processing issues you might want to address through your scheme. You should carry out research and consultation within your proposed target market to ensure that your scheme meets a need and will have market viability;

The client data file is at the heart of the legal industry and contains significant amounts of personal data. The processing of this file and the associated necessary protections are the focus for the LOCS:21 standard.

As described in the introduction above, research and consultation within the Legal Industry has been extensive based on experience and the introduction of an earlier standard focussed on Information Security.

where is there a need for enhanced trust;

LSPs receive an increasing amount of Security Questionnaires from corporate clients, all of which require demonstrative evidence of Information Security and Data Protection 'compliance'. In the absence of a recognised data protection certification the responses are varied and typically require a time consuming toing and froing of qualifying questions and answers.

For the general public, there is no recognisable assurance available.

how a particular processing activity impacts data subjects and how the proposed criteria or scheme would help them;

It is clear from consumer activity in areas such as food standard certificates on restaurant windows or kite marks on certain products that there is a desire for reassurance and confidence in the product consumed. Aside from the Lexcel certification which only lightly touches on data protection the Legal Industry offers no such reassurance even though significant amounts of personal data are being processed. Data Subjects often use law firms because they have to and simply trust that their data will be protected and processed appropriately.

LOCS:21 if approved by the ICO would become the 'kite mark' for Legal Service Providers and ensure three core fundamentals for dat subjects

1 Their data is protected adequately

2 The organisation recognises data subject rights and has the processes to enable them

3 If a data breach occurred the organisation has the appropriate process in place to manage and remediate the breach

4 The organisation will only share the data subjects data when appropriate and if acceptable protections are in place

how will the scheme documentation (including any logo, seal or mark) ensure that people can easily and immediately understand what is being certified and what that means for them;

Once approved by the ICO, the standard is likely to well adopted by Legal Service Providers as it is in their interest to promote consumer confidence. Over time and with wider adoption the LOCS:21 logo will be recognised by consumers, both corporate and the general public, as an indication that the organisation has had to demonstrate compliance with data protection standards.

The standard has the binary pass criteria pass or fail. and therefore avoids grades of pass (e.g. Distinction, Merit, etc) as these can be confusing and in our view do not help data subjects.

what schemes are already available; and

There are no ICO approved Certification Schemes currently available as applicable to the protection of client data in the Legal Services industry. The Law Society has a Lexcel Certification Scheme which focuses on general law firm management but only touches on data protection.

the name of the scheme – does it accurately reflect the scope, and will it be understandable to users?

LOCS:21 was named specifically to play on the word 'lock' which is synonymous with security and enables the use of a recognisable lock icon in the logo. The full name **L**egal Services **O**perational Privacy **C**ertification **S**cheme describes the market intended as well as the core focus – operational privacy.

LEGAL SERVICES OPERATIONAL PRIVACY CERTIFICATION SCHEME

AUGUST 2021 | **LOCS:21 STANDARD**

2TWENTY4 CONSULTING
DATA PROTECTION SERVICES

Contents

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 Sensitive Personal 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 must trust their own suppliers as sensitive personal 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 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 appropriate protections to 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 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 internal team'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 data breach or theft and a general industry desire to ensure the privacy and security of personal data when selecting third-party service providers. In addition, an expected outcome is that

The LOCS (Legal Services Operational Privacy Certification Scheme) accreditation is designed to:

- 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
- 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)

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 accreditation.

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

Scope

The primary processing activity within the scope of this standard is

Maintenance of the client data file

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

he LOCS:21 standard is applicable to any provider of Legal Services who wish to be LOCS:21 accredited. The LOCS standard is designed to ensure appropriate protection for the processing of Client Data by those services who maintain client files as would meet the UK GDPR requirements.

In addition, the above organisations may use Data Processors or Sub-Processors in their supply chain to assist with or provide processing services. To ensure complete protection across the Legal Service supply chain, these should be included within scope where applicable.

Legal Service Providers, and their supplier/Vendors/Solution providers that can demonstrate compliance with the LOCS:21 standard are entitled to use the LOCS:21 logo on their promotional material.

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 storage, data usage, 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 rights to object;
- Internal Governance
- Supply chain sub-contracting of processing activities
- Communicating with clients

Types of Organisations in Scope

The scope of the LOCS:21 accreditation covers any of the following types of organisation acting as a data controller, joint data controller or processor, that carry out any of the processing activities in 'Processing Activities in scope':

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

Processors and/or Sub-processors that assist with the general processing of Client Data may include:

- 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)

Processing Activities in Scope

To be eligible for certification against the LOCS:21 standard, applicants shall be maintaining client data files and carrying out one or more of the following data processing activities:

- Collection of client personal data;
- Storage of client personal data whether long term or transient;
- Modification of client data;
- 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;

Target of Evaluation

This Standard assesses the protective measures afforded to personal data by Legal Service Providers. The applicant for LOCS:21 accreditation 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.

Processes in scope will undertake activities listed in 'Processing Activities in Scope' listed above and may include (but not be limited to) customer engagement, document modification services, content storage, asset management, security, translation, transcription, consultancy, project implementation and IT support.

An applicant for LOCS:21 accreditation will be required to document the processing activities being presented for certification in terms of the types of data being processed (e.g., special category data, biometric data, etc.), as well as the systems and processes used.

The applicant will also be required to provide details of the following:

- Location of processing
- Sub-processors used
- Internal governance structure
- Existing relevant certifications

Territorial Scope for LOCS

The LOCS:21 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 relate to the offering of legal services (even if for free) to data subjects situated in the United Kingdom.

Normative References

Legal Services Operational Privacy Certification Scheme (LOCS)

LOCS:21:STANDARD – LOCS:21 detail of controls

LOCS:21:AUDIT SCHEDULE – Internal audit requirements for LOCS:21 standard

LOCS:21:CERTIFICATION CRITERIA – Certification Criteria for LOCS:21 standard

Legal Provisions

- Data Protection Act 2018S 2:2021
- 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.

Related National Standards

- ISO 27001:13
- Lexcel
- Cyber Essentials

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/

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;

Guidance Notes, including checklists produced and published by the UK Information Commissioner's Office;

WP29 – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679;

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 for identifying a controller or processor's lead supervisory authority;

WP29 – Guidelines on the right to data portability;

WP29 – Guidelines on consent under Regulation 2016/679;

WP29 – Guidelines on transparency under Regulation 2016/679;

WP29 – Opinion 02/2012 on facial recognition in online and mobile services (WP 192);

United Kingdom's Data Ethics Framework (updated 30th August 2018).

Definitions

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

'Client' The user of legal services from a Legal Service Provider

'Data Breach' means the loss, corruption or non-availability of personal data

'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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

'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

'ICO' means the Information Commissioners Office

'Joint Controller' Where two or more Data Controllers share obligations and responsibilities for the Processing of Personal Data

'**Legal Service Provider'** means an organisation that offers legal services to clients

'Legal Service Provider Supplier' means an organisation that offers services to Legal Service Providers

'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

'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

'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

'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.

Compliance Requirements

LOCS:21 uses the following compliance requirement terms:

MUST	this is mandatory to achieve the **LOCS:21** accreditation
MUST(G)	this is mandatory to achieve the **LOCS:21** accreditation and mandatory under UK GDPR.
SHOULD	this is not required to achieve the **LOCS:21** accreditation but constitutes current best practice.
OPTION	this describes something that may be applied but is not required to achieve the **LOCS:21** accreditation.

Methodology

The **LOCS:21** 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 four core areas for assessment:

- **Governance**
- **Operational Privacy**
- **Monitoring & Review**
- **Continuous Improvement**

To ensure a maintained compliance effort, the framework includes a mandatory self-audit program. Evidence of the previous year's self-audit will be required for all renewals of the **LOCS:21** certification.

For Applicant Organisations to achieve LOCS:21 accreditation, the following steps will apply:

1. **Ensure the organisation meets the processing criteria defined in the 'Scope' section**
2. **Download the LOC:21 documentation from the ICO website**
3. **Ensure all controls are in place and can be evidenced**
4. **Provide evidence that the controls have been met to a satisfactory level to an approved LOCS:21 assessor**
5. **Assessor will provide initial review and determine whether any further action is required to meet the certification criteria.**
6. **If necessary, provide evidence of additional actions**
7. **Final assessment and Certification approved where pass criteria has been met.**

The assessor will use the following assessment criteria for each control:

- **Not met –** there is insufficient evidence that this control is in place
- **Partially Met –** there is some evidence that this control is in place but further action is required
- **Compliant –** there is evidence this control is in place and meets acceptable levels

Applicant Organisations must meet 100% Compliance of **MUST(G)** controls and 80% of all other controls to achieve certification.

Where a control is only Partially Met the assessor will advise as to any mitigations or required improvements.

Certification will be assessed and provided by an approved **LOCS:21** Assessor.

Controls Table

The **LOCS:21** standard includes the following assessed controls:

CONTROL CATEGORY	CONTROL	CONTROL NAME	REQUIREMENT LEVEL
GOVERNANCE	LOCS:21:C1	Scope Detail	**MUST**
GOVERNANCE	LOCS:21:C2	Privacy Council	**MUST**
GOVERNANCE	LOCS:21:C3	DPO decision	**MUST (G)**
GOVERNANCE	LOCS:21:C4	Data Protection Policy	**MUST (G)**
GOVERNANCE	LOCS:21:C5	Acceptable Use Policy	**MUST**
GOVERNANCE	LOCS:21:C6	User Account Policy	**MUST**
GOVERNANCE	LOCS:21:C7	Removable Device Policy	**MUST**
GOVERNANCE	LOCS:21:C8	Service Procurement Policy	**MUST**
GOVERNANCE	LOCS:21:C9	Remote Access Policy	**MUST**
GOVERNANCE	LOCS:21:C10	Business Continuity Policy	**MUST**
GOVERNANCE	LOCS:21:C11	Retention Policy	**MUST (G)**
GOVERNANCE	LOCS:21:C12	Destruction Policy	**MUST**
OPERATIONAL PRIVACY	LOCS:21:C13	DPIA Form	**MUST (G)**
OPERATIONAL PRIVACY	LOCS:21:C14	Record of Processing Activities (ROPA)	**MUST (G)**
OPERATIONAL PRIVACY	LOCS:21:C15	Lawful Processing	**MUST**
OPERATIONAL PRIVACY	LOCS:21:C16	Risk Register	**MUST**
OPERATIONAL PRIVACY	LOCS:21:C17	Supplier Register	**MUST**
OPERATIONAL PRIVACY	LOCS:21:C18	Supplier Adequacy Checklist	**MUST (G)**
OPERATIONAL PRIVACY	LOCS:21:C19	Supplier Data Protection Agreement	**MUST (G)**
OPERATIONAL PRIVACY	LOCS:21:C20	Standard Contract Clauses	**MUST (G)**
OPERATIONAL PRIVACY	LOCS:21:C21	Privacy Notice	**MUST**
OPERATIONAL PRIVACY	LOCS:21:C22	Employee Privacy Notice	**MUST (G)**
OPERATIONAL PRIVACY	LOCS:21:C23	Breach Register	**MUST (G)**
OPERATIONAL	LOCS:21:C24	DSAR Register	**MUST**

PRIVACY			
OPERATIONAL PRIVACY	LOCS:21:C25	Technical Measures	**MUST**
OPERATIONAL PRIVACY	LOCS:21:C26	Organisational Measures	**MUST**
OPERATIONAL PRIVACY	LOCS:21:C27	Data Subject Rights	**MUST (G)**
OPERATIONAL PRIVACY	LOCS:21:C28	Breach Report Form	**MUST**
OPERATIONAL PRIVACY	LOCS:21:C29	SAR Request Form	**MUST**
MONITORING & REVIEW	LOCS:21:C30	Control Audit Schedule	**MUST**
CONTINUOUS IMPROVEMENT	LOCS:21:C31	Training Log	**MUST (G)**

LOCS:21 Controls

1. GOVERNANCE

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

1.1. Scope & Objectives

CONTROL LOCS:21:C1
Governance - Scope Detail

The organisation MUST determine the scope of the LOCS accreditation by documenting the following:

- Geographies within scope
- Offices within scope
- Systems within scope
- Organisational objectives for personal data management

AUDIT REFERENCE	LOCS2:21:A1 – Scope Document

1.2. Responsibility & Accountability

1.2.1. Privacy Council

CONTROL LOCS:21:C2
Governance - Privacy Council

- The organisation MUST create a Privacy Council that will take overall responsibility for data protection activities
- The Privacy Council MUST include the most senior IT professional and at least one of the non-IT Senior Management team.

AUDIT REFERENCE	LOCS2:21:A2 – PRI CON

1.2.2. Data Protection Officer

CONTROL LOCS:21:C3
Governance - DPO decision

- The organisation MUST(G) determine whether a Data Protection Officer (DPO) is required under the UK GDPR or local legislation.

- The organisation MUST(G) document the decision process
- If a DPO is not required by legislation the organisation MUST either voluntarily appoint a DPO or appoint an alternative manager of Data Protection.
- The organisation SHOULD give the manager of Data Protection similar status to that of a DPO within the organisation.

AUDIT REFERENCE	LOCS2:21:A3 – DPO Document

UK GDPR REFERENCE	Articles 37 - 39

1.2.3. Registration

- If the organisation is based in the UK and if it processes personal data it MUST(G) register with the Data Protection Authority (ICO).
- If the organisation is based in the UK and if it has appointed a DPO it MUST register the DPO with the Data Protection Authority.

1.3. Data Protection Principles

All organisations MUST(G) apply the following data protection principles to all personal data processing activities:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**');
- it is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
- it is all accurate and, where necessary, kept up to date and that reasonable 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**');
- it is 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**');
- it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

1.4. Data Protection Policy

CONTROL LOCS:21:C4
Governance – Data Protection Policy

- The organisation MUST(G) have a documented Data Protection Policy.
- The organisation MUST (G) make the Data Protection Policy available to all employees.
- The organisation SHOULD audit employee absorption of the policy.

GUIDANCE
The overall Data Protection Policy should include at a minimum the headings in sections 1.4.1 to 1.4.8 although these may also exist as separate policies if required.

AUDIT REFERENCE	LOCS2:21:A4 – Policy Documents

1.4.1. Acceptable Use Policy

- The organisation MUST have an Acceptable Use policy.
- The policy MUST at a minimum describe acceptable usage of organisation systems by employees.

CONTROL LOCS:21:C5
Governance - Acceptable Use Policy

1.4.2. User Account Policy

- The organisation MUST have a User Account policy.
- The policy MUST at a minimum define organisation rules for system account roles and access rights.

CONTROL LOCS:21:C6
Governance - User Account Policy

1.4.3. Removable Device Policy

- The organisation MUST have a Removable Device policy.
- The policy MUST at a minimum define organisation rules for use of devices that are removed from the office location

CONTROL LOCS:21:C7
Governance - Removable Device Policy

1.4.4. Service Procurement Policy

- The organisation MUST have a Service Procurement policy.
- The policy MUST at a minimum describe the organisation's rules for procuring new services.
- New services procured that will process high risk personal data MUST(G) be accompanied by a DPIA (see 2.1)

CONTROL LOCS:21:C8
Governance - Service Procurement Policy

1.4.5. Remote Access Policy

- The organisation MUST have an Remote Access policy.
- The policy MUST at a minimum describe the organisation's rules for employees working remotely.

CONTROL LOCS:21:C9
Governance - Remote Access Policy

1.4.6. Business Continuity Policy

- The organisation MUST(G) have a Business Continuity policy.
- The policy MUST at a minimum include a Business Continuity Plan, a Communication Plan and a Test Plan.

CONTROL LOCS:21:C10
Governance - Business Continuity Policy

1.4.7. Retention Policy

- The organisation MUST(G) have a Retention Policy.
- The policy MUST(G) reference all personal data being processed.
- The policy MUST(G) be referenced in the organisation's Privacy Notices (see 3.7)

CONTROL LOCS:21:C11
Governance - Retention Policy

1.4.8. Destruction Policy

- The organisation MUST have a Destruction Policy.
- The policy MUST include the organisation's rules for destroying paper and electronic data.

CONTROL LOCS:21:C12
Governance - Destruction Policy

2. OPERATING 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 adequately protected.

2.1. Data Protection Impact Assessment (DPIA)

CONTROL LOCS:21:C13
Operational Privacy - DPIA Form

- You MUST(G) provide a DPIA template for internal use.
- The template MUST(G) be published and available to all department heads or others that may introduce process change.
- A DPIA MUST(G) be provided for all changes to internal processes or systems that involve a high risk to personal data.

GUIDANCE
Successfully embedded within the organisation the DPIA can be one of the most effective ways to communicate change and enable the DPO (1.2.2) or person responsible for data protection to take associated actions such as updating the risk register (2.4), updating processing records (2.2) and maintain the Supplier Register (2.5)

AUDIT REFERENCE	LOCS2:21:A5 – DPIA Document

UK GDPR REFERENCE	Article 35

2.2. Processing Records

CONTROL LOCS:21:C14
Operational Privacy - Record of Processing Activities (ROPA)

- The organisation MUST(G) document all areas of processing that involve personal data.
- The organisation MUST(G) maintain these records.
- This record shall contain:
- Core details of each processing activity
- Lawful basis applied to that activity
- Retention period applied to data associated with that activity.
- Details where applicable of the Data Protection Officer.
- Categories of processing carried out on behalf of clients.
- Where applicable detail of transfers to any third country.
- Where possible a general description of the technical and organisational security

measures which could include reference to appropriate policies and certifications held.

GUIDANCE
To meet the LOCS requirement processing records are mandatory. The GDPR however provides exceptions for organisations under 250 in size in limited circumstances. (see GDPR Art 30.5)

AUDIT REFERENCE	LOCS2:21:A6 – ROPA

UK GDPR REFERENCE	Article 30

2.3. Lawful Processing

CONTROL LOCS:21:C15
Operational Privacy – Lawful Processing

- The organisation MUST(G) indicate the UK GDPR Art 6 (see 2.3.1) lawful basis it is relying on for any personal data being processed.
- The organisation MUST(G) indicate the UK GDPR Art 9 (see 2.3.1) lawful basis it is relying on for any special category data being processed.

GUIDANCE
A good place to register the lawful basis for processing personal data is in the Record of Processing Activities (see 2.2)

AUDIT REFERENCE	LOCS2:21:A7 – Lawful Basis

UK GDPR REFERENCE	Article 6 & Article 9

2.3.1. UK GDPR Lawful Processing Principles

The UK GDPR Art 6 lawful basis for processing personal data:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
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;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
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;
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.

The UK GDPR Art 9 lawful basis for processing special category data:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
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 Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
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;
d) processing is carried out in the course of its legitimate activities with appropriate 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;
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State 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;
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 Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
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 Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
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) based on Union or Member State 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.

2.4. Risk Register

CONTROL LOCS:21:C16
Operational Privacy - Risk Register

- The organisation MUST create and maintain a register of any risks to Data Protection.
- The organisation MUST determine a risk classification system (e.g. High, Medium, Low)
- The organisation MUST indicate mitigation steps for these records.

GUIDANCE
The Risk Register must be kept updated as new risks occur or mitigations actioned. The DPIA (see 2.1) is a good mechanism for identifying new risks.

AUDIT REFERENCE	LOCS2:21:A8 – Risk Register

2.5. Supplier Register

CONTROL LOCS:21:C17
Operational Privacy - Supplier Register

- The organisation MUST(G) document all third-party suppliers that process personal data.
- The organisation MUST(G) maintain these records.

AUDIT REFERENCE	LOCS2:21:A9 – Supplier Register

2.5.1. Supplier Risk Assessment

The organisation SHOULD assess their suppliers using the following criteria:

- Is special category data being processed?
- Are large volumes of personal data being processed?
- Are they processing outside of the EEA?
- Is the supplier critical to our organisation?

If any of these criteria are met the supplier SHOULD be designated as 'high risk' and either a Data Processing Agreement (if Processor – see 2.6.2) or Statement of Adequacy obtained (if Controller – see 2.6.1)

2.6. Third Party Data Transfer

2.6.1. Controller to Controller

CONTROL LOCS:21:C18
Operational Privacy - Supplier Adequacy Checklist

- If data is being transferred to another Data Controller, a Statement of Adequacy MUST be requested.

GUIDANCE
Although it is a LOCS requirement to request an adequacy statement from Data Controllers processing an organisations data, they may not respond. In this case the DPO (or equivalent) should assess the risk to proceed.

AUDIT REFERENCE	LOCS2:2:A10 – Adequacy Checklist

2.6.2. Controller to Processor

CONTROL LOCS:21:C19
Operational Privacy - Supplier Data Protection Agreement

- If data is being transferred to a Data Processor, a Data protection Agreement MUST(G) be agreed by both parties unless the standard contract terms have equivalent data protection provisions.

GUIDANCE
Although it is a LOCS and a UK GDPR requirement to have a documented Data Processing Agreement agreed by both parties, for larger suppliers (Microsoft, Amazon etc) it may be that a published statement on their website is all that is available. In this case the DPO (or equivalent) should assess the risk to proceed.

AUDIT REFERENCE	LOCS2:21:A11 – DPA

UK GDPR REFERENCE	Article 28

2.6.3. Joint Controller

- If two organisations in a data transfer relationship both determine the means and purposes of the processing they can establish themselves as Joint Controllers.
- If an organisation is a Joint Controller it MUST(G) agree and document shared roles and responsibilities with the other party.
- A Joint Controller MUST(G) make the documented roles and responsibilities available to the Data Subject.

GUIDANCE
If Joint Controller status is agreed it is worth noting that the data subject may exercise his or her rights under GDPR in respect of and against each of the controllers.

UK GDPR REFERENCE	Article 26

2.6.4. Transfer outside of the UK or EEA

CONTROL LOCS:21:C20
Operational Privacy - Standard Contract Clauses

If an organisation intends to transfer data outside of the UK or EEA it MUST(G) use one of the following legal justifications:

- Recipient organisation is located in a nation state named in the EU and/or UK Adequacy List subject to article 45 of Regulation (EU) 2016/679.
- A Standard Contract Clause pursuant to article 45 of Regulation (EU) 2016/679 or the ICO Standard Contract Clauses for UK data.
- Binding Corporate Rules ratified by the ICO
- Any such transfer legalised by one of the above measures MUST(G) be made transparent to the Data Subject (see Privacy Notice 2.7)

GUIDANCE
Consent from the individual Data Subject can be used as an exception to the above three criteria although should only be used in exceptional circumstances and temporarily.

AUDIT REFERENCE	LOCS2:21:A12 – INTTRAN

UK GDPR REFERENCE	Articles 44-50

2.7. Privacy Notices

2.7.1. Data Subject Privacy Notice

CONTROL LOCS:21:C21
Operational Privacy - Privacy Notice

An organisation MUST(G) publish a notice or policy that describes processing activity. The notice or policy MUST(G) include the following information.

- The name and contact details of our organisation.
- The name and contact details of our Data Protection Officer or alternative representative
- The purposes of the processing.
- The lawful basis for the processing.
- The categories of personal data obtained
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

An organisation MUST(G) make the privacy policy or notice available to data subjects at the time of data collection or if obtained from a source other than the individual it relates to:

- within a reasonable period of obtaining the personal data and no later than one month;
- at the latest, when the first communication takes place; or
- if disclosed to someone else, at the latest, when the data is disclosed

An organisation SHOULD when providing privacy information to individuals, use a combination of appropriate techniques, such as:

- a layered approach;
- dashboards;
- just-in-time notices;
- icons; and
- mobile and smart device functionalities.

GUIDANCE
Effective use of the Privacy Notice on your website is a good way to deliver the transparency of processing that data protection legislation requires. For transactions that are not website related alternative means of delivering the information to the data subject are required.

AUDIT REFERENCE	LOCS2:21:A13 – Privacy Notice

UK GDPR REFERENCE	Articles 12-13

2.7.2. Employee privacy Notice

CONTROL LOCS:21:C22
Operational Privacy - Employee Privacy Notice

An organisation MUST publish a notice or policy that describes the processing activity of employee data. The notice or policy MUST include the following information.

- The name and contact details of our Data Protection Officer or alternative representative
- The purposes of the processing.
- The lawful basis for the processing.
- The categories of personal data obtained.
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data during and post-employment.
- The rights available to individuals in respect of the processing.
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).

- The details of the existence of automated decision-making, including profiling (if applicable).

An organisation MUST make the privacy policy or notice available to employees prior to employment or at the time of data collection.

GUIDANCE
An employee privacy notice should make reference to the organisation's acceptable use policy and indicate what happens to personal data on the organisation's systems post employment.

AUDIT REFERENCE	LOCS2:21:A14 – Employee Privacy Notice

2.8. Incident Registers

2.8.1. Breach Register

CONTROL LOCS:21:C23
Operational Privacy - Breach Register

An organisation MUST maintain a register of all internal data breaches.

An organisation MUST collect the following information for reported data breaches:

- The date and time the breach was made known to the organisation
- The date and time the breach occurred.
- The name of the individual or supplier reporting the breach
- The nature of the data breach
- The categories and approximate number of data subjects concerned
- The categories and approximate number of data records concerned;
- Describe the likely consequences of the data breach;
- Describe the measures taken or proposed to be taken by the controller to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

GUIDANCE
For a detailed explanation the term 'data breach' for personal data see the Article 29 Working Party 'Guidelines on Personal data breach notification under Regulation 2016/679'

AUDIT REFERENCE	LOCS2:21:A15 – Breach Register

2.8.2. DSAR Register

CONTROL LOCS:21:C24
Operational Privacy - DSRR Register

An organisation MUST maintain a register of all Data Subject Right Requests.

An organisation MUST collect the following information for Subject Access Requests:

- Date of request
- Type of request
- Name
- Contact details
- Data requested
- Identity confirmed
- Actions taken
- Date concluded

AUDIT REFERENCE	LOCS2:21:A16 – SAR Register

2.9. Technical & Organisational Measures

2.9.1. Technical measures

CONTROL LOCS:21:C25
Operational Privacy – Technical Measures

2.9.1.1. Systems Map

An organisation MUST document the core business systems indicating the following:

- how they interact
- data flow
- type of data present
- system owner
- on/off premises
- Access control

AUDIT REFERENCE	LOCS2:21:A17 – Systems Map

2.9.1.2. Patch Management

- An organisation MUST have a documented procedure for applying system patches and updates.

AUDIT REFERENCE	LOCS2:21:18 – Patch Procedure

2.9.1.3. Removable Device Protection

- An organisation MUST enable the encryption of data on removable devices including but not limited to, laptops, memory sticks and external drives.
- An organisation's measures MUST reference and reflect its Removable Device Policy (see 1.3.3)

AUDIT REFERENCE	LOCS2:2:A19 – RDP

2.9.1.4. Gateway Protection

An organisation MUST protect its technology environment by implementing at least the following:

- Firewalls
- Anti-Virus/Malware
- Network Access Security
- Penetration Tests

An organisation SHOULD protect its technology environment by implementing at least the following:

- Data Leakage Protection
- Multi Factor Authentication
- Threat Detection

AUDIT REFERENCE	LOCS2:21:A20 – Gateway Protection

2.9.1.5. User Access

- An organisation MUST enforce a strong password model for system access.
- An organisation's measures MUST reference and reflect its User Account Policy (see 1.3.2)

AUDIT REFERENCE	LOCS2:21:A21 – User Access

2.9.1.6. Security Solution Register

- An organisation SHOULD document all systems and solutions that are in place to help protect data.

AUDIT REFERENCE	LOCS2:21:A22 – Security Solutions Register

2.9.2. Organisational Measures

CONTROL LOCS:21:C26
Operational Privacy – Organisation Measures

2.9.2.1. Access Control

An organisation MUST apply role-based access to its systems

AUDIT REFERENCE	LOCS2:21:A23 – Role Based Access Control

2.9.2.2. Asset Management

An organisation MUST keep a record of all its technology assets.

The Asset record MUST include at a minimum:

- Device Name
- Device Type
- Serial No
- MAC address (if appropriate)
- Primary User

AUDIT REFERENCE	LOCS2:21:A24 – Asset Register

2.9.2.3. Secure Disposal

- An organisation MUST delete data to a minimum of Department of Defence standard prior to disposing of electronic equipment.
- An organisation MUST dispose of paper documents and files by shredder or confidential waste.

AUDIT REFERENCE	LOCS2:21:A25 – Secure Disposal

2.9.2.4. Disaster Recovery & Business Continuity

- An organisation MUST test their Business Continuity/Disaster Recovery Plan on an annual basis.
- An organisation SHOULD test their Business Continuity/Disaster Recovery Plan on a regular basis.
- An organisation's measures MUST reference and reflect its Business Continuity Policy (see 1.3.6)

AUDIT REFERENCE	LOCS2:21:A26 –DR/BC Test

2.10. Data Subject Rights

CONTROL LOCS:21:C27
Operational Privacy – Data Subject Rights

Where an organisation is a Data Controller it MUST(G) provide the following rights detailed in 2.10.1 – 2.10.7 to data subjects:

AUDIT REFERENCE	LOCS2:21:A27 – DS Rights

UK GDPR REFERENCE	Articles 12 -23

2.10.1. Right to Information

The data subject has the right to be informed as to elements of how its data will be processed. (See 2.7 Privacy Notices)

2.10.2. Right of Access

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- 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;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- 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;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- 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

2.10.3. Right to Rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her

2.10.4. Right to Erasure

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- 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;
- 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);
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
-

2.10.5. Right to Restriction of Processing

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller 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;
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2.10.6. Right to Data Portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on consent or on a contract
- the processing is carried out by automated means

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

2.10.7. Right to Object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

2.11. Incident management

2.11.1. Data Breach management

CONTROL LOCS:21:C28
Operational Privacy - Breach Report Form

- An organisation MUST have a defined and published breach reporting process.
- An organisation MUST make all employees aware of the breach reporting process
- An organisation MUST(G) report ‘material’ personal data breaches to the Data Protection Authority within 72 hours.

GUIDANCE
‘material’ requires an assessment as to whether a data breach has the potential to impact

the rights and freedoms of the data subject.

AUDIT REFERENCE	LOCS2:21:A28 – Breach Reporting Documentation

2.11.2. Data Request Management

CONTROL LOCS:21:C29
Operational Privacy - SAR Request Form

- An organisation MUST provide a SAR Request Form for any subject access requests received.
- An organisation MUST make all employees aware of the SAR reporting process
- An organisation MUST(G) respond to the Data Subject within 30 days.
- An organisation SHOULD refer to an internal SAR Checklist.

AUDIT REFERENCE	LOCS2:21:A29 –SAR Documentation

2.12. Physical Security

An organisation MUST(G) give paper documents and files adequate protection including but not limited to:

- Secure physical storage
- Access control
- Defined retention period
- Controlled destruction

An organisation SHOULD consider a clear desk policy.

3. MONITOR & REVIEW

This section describes the controls designed to enable certification applicants to demonstrate that they are monitoring the implementation of the LOCS:21 controls through the use of regular audits.

3.1. Internal Audit

3.1.1. Audit Process

CONTROL LOCS:21:C30
Monitor & Review - Control Audit Schedule

AUDIT REFERENCE	LOCS2:21:A30 – CAS

An organisation MUST have a documented Control Audit Schedule.

The schedule MUST use the LOCS format and set its own parameters for the following.

- Control Audit Frequency
- Control Owner
- Audit Sign Off

The schedule MUST be reviewed by the Security Council (1.2.1) and at Management Review meetings (3.2).

3.2. Management Review

- An organisation MUST carry out management review meetings with Security Council members in attendance on a regular basis.
- An organisation SHOULD carry out a monthly review of the LOCS audit schedule and risk register.

3.3. External Audit

- An organisation can as an OPTION engage an external consultant to audit compliance with the LOCS accreditation.

4. CONTINUOUS IMPROVEMENT

This section describes the controls designed to enable certification applicants to demonstrate that through the use of corrective and preventative measures they are seeking to maintain and improve their accountability. The continued training of employees will lead to greater awareness and continuous improvement.

4.1. Corrective Measures

- An organisation MUST introduce measures to respond to issues and/or risks encountered.
- An organisation MUST log all new risks in the Risk Register.
- An organisation MUST recommend mitigations for logged risks.
- An organisation MUST log all issues in the Issues Log of the Risk Register
- An organisation MUST recommend mitigations for logged issues.

4.2. Preventative Measures

- An organisation MUST monitor system logs for suspicious activity
- An organisation MUST undergo penetration tests at least annually
- An organisation MUST provide Information Security and Data Protection best practice training for users of their systems.

4.2.1. User Training

CONTROL LOCS:21:C31
Continuous Improvement – User Training Log

- An organisation MUST have a documented User Awareness Programme
- The User Awareness Programme MUST include an auditable reference of training delivered and attended.

GUIDANCE
It is recommended that the User Awareness Programme is delivered using multiple channels (presentations, e-learnings, posters, communications etc) and delivered as a series of events over a calendar year.

AUDIT REFERENCE	LOCS2:21:A31 – UAP

Tim Hyman - DPO for hire. Background in legal sector working with them towards GDPR compliance.

Pillar 9 assessment - NATO etc not subject to GDPR (?) - this was a way of EU certifying they had certain safeguards in place.
International fund for development - worked with them.
Realised certification really useful - B&W indication of compliance.
Supply chain will benefit from certification for enhanced trust. Helps provide assurance.

Don't want to be CB.

Will provide feedback.

From:	certification
To:	timhyman@2twenty4consulting.com
Bcc:	Lewis Behan; Christine Eckersley
Subject:	Information Commissioner"s Office: Feedback on LOCS:21 UK GDPR scheme criteria
Date:	29 October 2021 17:00:00
Attachments:	image001.jpg 224 LOCS Certification criteria TRIAGE 20211029.docx

Dear Tim

We have now had the chance to review the UK GDPR certification criteria in the **Legal Services Operational Privacy Certification Scheme Standard** document, submitted on 25 August 2021.

Please find our feedback in the attached triage form. As discussed in our recent meeting, we felt that it was a good start and the fundamental building blocks are there. However, at this stage it unfortunately does not meet our initial requirements.

I hope the attached feedback is helpful but please let me know if you have any questions or want to discuss anything - I am happy to arrange a call.

Kind regards,

Sarah

Logo

Sarah Carr

Senior Case Officer (Codes & Certification) - Assurance

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6750 F. 01625524510 ico.org.uk
twitter.com/iconews Livechat

Certification scheme triage form

Certification scheme title	Legal Services Operational Privacy Certification Scheme (LOCS:21)
Details of scheme owner: • **name and acronym** • **legal entity** • **physical address** • **web address**	2twenty4Consulting Ltd 70 Croft Road Hastings TN34 3HE Limited company. Companies House reg: 07755609 ICO reg: ZA377863 www.2twenty4consulting.com
Main contact details for queries re submission.	Tim Hyman 07500227009 timhyman@2twenty4consulting.com
Date submitted	24/08/2021
Territorial scope	UK and organisations subject to UK GDPR
Details of any other countries where the criteria have been/will be submitted for approval	N/A
Have potential certification bodies been identified at this point?	Not seeking accreditation themselves. No potential CBs been identified.

Requirement	**Yes / No / Partially**	Comments	Recommendation
1. Supporting documentation included *(Request if not provided)*			
Scheme criteria catalogue	Yes	**LOCS Certification Standard** sets out the certification criteria.	-
Use case (unless included in criteria catalogue)/testing	Partially	**LOCS Certification Scheme Application** document explains they have worked with legal firms to test the scheme and the	-

		original PROSEC2.0 standard. No evidence/results provided.	
Rationale for scheme and intended audience (unless included in criteria catalogue)	Yes	Covered in the **LOCS Certification Scheme Application** and the introduction of the **LOCS Certification Standard.** Originally developed a standard, PROSEC2, which some law firms adopted. LOCS:21 builds on that with the intention that it improves DP compliance and provides enhanced trust for data subjects.	-
2. General format			
Laid out in logical and understandable way (sections clearly identifiable, clauses numbered, appropriate language used)	Partially	**LOCS Certification Standard** This is the main document setting the data protection requirements. Key sections of the document are not numbered. In the Controls section, subsections are numbered but not the individual requirements. This makes it difficult when referencing the relevant requirements, including cross-referencing within the document.	Apart from the introduction all other sections should be numbered, eg 1. Scope 2. Normative references 3. Terms and definitions 4. Data protection requirements With appropriate subsections within each. For ease of reference, make sure each separate requirement is numbered. For example: 2.4 Risk Register 2.4.1 The organisation shall create and maintain a register of any risks to Data Protection. 2.4.2 The organisation shall determine a risk classification system (e.g. High, Medium, Low) 2.4.3 The organisation shall indicate mitigation steps for any risks. You can look at other ISO standards for how the document should be structured. It might also be helpful to look at BSI Rules for the structure and drafting of UK standards or ISO/IEC Directives, Part 2 — Principles and

			rules for the structure and drafting of ISO and IEC documents
		There are two key documents: **LOCS Certification Standard** and **LOCS Assessment Criteria**. This is a little confusing as UK GDPR refers to 'certification criteria' as the requirements but assessment criteria document seems to be setting out what evidence must be provided to auditors. There is also some duplication in this document to what appears in the Standard. There is also then an audit checklist, but this appears to be for applicants to use rather than the scheme auditors. Certification schemes consist of three key elements: • The **criteria outlining specific data protection requirements**. These form the 'standard' against which the conformity of a product or service is assessed. • The **audit methodology and testing methods** that are used by the certification body to carry out that assessment. This is usually developed by the certification body, but the scheme owner may need to set certain requirements for auditors as necessary. • The **scheme manual**. This is the document that sets out how the scheme operates. Again this is usually a document developed by the certification body operating the scheme.	Consider what each document's purpose is and that titles make that clear.

		There are references throughout to 'accreditation' when in fact it is referring to the certification process. For example, paragraph 4 of the scope section says, *"the LOCS:21 standard is applicable to any provider of Legal Services who wish to be LOCS:21 accredited."* Accreditation is the process that the certification body goes through in order to be approved by UKAS to operate a certification scheme and certify organisations against that scheme.	Replace references to accreditation/accredit/accredited with certification/certify/certified as appropriate.
		There are some elements of the **LOCS Certification Standard** that refer to information that will be part of the certification process and therefore up to the certification body operating the scheme, eg in the **'methodology' section** on **p.10**.	Make sure that the standard is not setting requirements that would normally be set by the accredited certification body.
		The **'methodology' section** also says, *"Applicant Organisations must meet 100% Compliance of **MUST(G)** controls and 80% of all other controls to achieve certification."* Which is unlikely to be compatible with ISO 17065 which requires 100% compliance with the mandatory criteria.	Ensure any requirements are compatible with ISO 17065.
		Point 1 in the **methodology section** says, *"Ensure the organisation meets the processing criteria defined in the 'Scope' section".* This wording might be confusing as we would assume the processing criteria are the data protection requirements set out in the standard.	Consider terminology used and ensure it is consistent and not confusing.
Uses specific non-subjective language (eg shall/should. Avoids use of non-specific terms, eg 'appropriate'.)	Partially	The **LOCS Certification Standard** uses 'MUST' to indicate requirements. The following verbal forms are the accepted standard in normative documents used in certification:	When setting requirements in the Standard replace 'must' with 'shall'. See section 7.2 – 7.6 of BSI Rules for the structure and drafting of UK standards or ISO/IEC Directives, Part 2 — Principles and rules for

		Requirements: shall/shall not Recommendations: should/should not.	the structure and drafting of ISO and IEC documents
		There is some use of non-specific language such as 'appropriate'. Section 5.2.9 of 'ISO 17007 Conformity assessment – guidance for drafting normative documents suitable for use for conformity assessment' states: *"Specified requirements should be stated unambiguously using wording that is objective, logical, valid and specific. In particular,* - *terms such as "adequate", "adversely affected", "sufficiently strong" and "extreme conditions" are subjective and should be avoided;* - *qualitative nouns and adjectives that could be taken as absolute, e.g. "waterproof", "unbreakable", "flat", and "safe", should not be used unless defined;* - *qualitative nouns and adjectives that describe a measurable property, e.g. "high", "strong", "transparent", and "accurate", should not be used unless defined;* - *the term "unless otherwise specified" should not be used, except when the "other specification" is clearly identified in the requirements."* To be compatible with ISO 17065 the criteria need to meet these language requirements and set specific and auditable data protection requirements.	Make sure that criteria set objective, specific and measurable data protection requirements for the processing, avoiding the use of non-specific language.
Normative references identified	Yes	Normative references section - **LOCS Certification Standard, p.7-8.** Refers to Related National Standards and lists ISO 27001:13, Lexcel, and Cyber Essentials, but does not give any details of what these standards are.	Provide corresponding title of the standards, eg ISO 27001:13 - Information technology - Security techniques - Information security management systems – Requirements, or a brief explanation of what the standard is. It may also be helpful to have a very brief

			explanation of how these relate, for example, are they referred to in the document? Are there requirements from them built into the LOCS standard?
Relevant terms defined	Partially	Some need aligning to UK GDPR, eg 'Data breach' says '*means the loss, corruption or non-availability of personal data'*, whereas the UK GDPR definition of a personal data breach in Article 4(12) goes further to say, "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."	Definitions of data protection related terms should be aligned to UK GDPR and/or ICO guidance to ensure the meaning is not diminished by simplifying the definition.
Introduction including background and motivation for the scheme, including how the criteria will improve data protection compliance and benefit data subjects.	Yes	**LOCS Certification Standard, p3:** *"In the absence of an approved Certification Scheme the users of legal services can only trust that Legal Service Providers are applying 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 internal team'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 data breach or theft and a general industry desire to ensure the privacy and security of personal data when selecting third-party service providers. In addition, an expected outcome is that* *The LOCS (Legal Services Operational Privacy Certification Scheme) accreditation is designed to:*	Incorporate information about the benefits to data subjects into the introduction section of the **LOCS Certification Standard.**

		• *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* • *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)* *…The LOCS accreditation is designed to assist and support any obligation to meet UK GDPR standards."* The **LOCS Certification Scheme Application** covers more about the benefits to data subjects. For example, it says. *"LOCS:21 if approved by the ICO would become the 'kite mark' for Legal Service Providers and ensure three core fundamentals for data subjects* *1 Their data is protected adequately* *2 The organisation recognises data subject rights and has the processes to enable them* *3 If a data breach occurred the organisation has the appropriate process in place to manage and remediate the breach* *4 The organisation will only share the data subjects data when appropriate and if acceptable protections are in place* *how will the scheme documentation (including any logo, seal or mark) ensure that people can easily and immediately understand what is being certified and what that means for them;"*	

		It may be beneficial to incorporate some of this information into the introduction of the Standard so that it clear to the reader how the LOCS standard benefits data subjects.	
3. Scope			
Name of the scheme is meaningful and not misleading to intended audience.	Yes	**LOCS Certification Scheme Application** *"LOCS:21 was named specifically to play on the word 'lock' which is synonymous with security and enables the use of a recognisable lock icon in the logo. The full name **L**egal Services **O**perational Privacy **C**ertification **S**cheme describes the market intended as well as the core focus – operational privacy."* YOUR DATA PROTECTED This name appears to be self-explanatory.	-
Scope clearly defined, meaningful and not misleading to intended audience.	Yes	**LOCS Certification Standard, Scope section, p.4-5** *"The primary processing activity within the scope of this standard is* ***Maintenance of the client data file"*** Sets out scope of standard, processing in scope, types of organisations in scope. Scope section also covers territorial scope and ToE.	-

		It appears to be clear what it is possible to certify and would not be misleading to intended audience.	
Scope reflects all relevant aspects of processing operations (eg. Privacy Health Mark must include all aspects of processing health data.)	Partially	Does not specifically say how UK GDPR applies. The opening sentence says *"Maintenance of the client data file"* – might be better to refer to the processing of personal data within the client data file which means UK GDPR applies.	Clarify how and why UK GDPR applies to the processing activity within scope.
		Refers to all aspects of processing operations when creating and maintaining the file. Although this is presented in a logical format, i.e. collection of personal data is the first bullet point and 'destruction of client data' it may be helpful to refer to the 'life cycle' of the data processing to make it clear why these aspects are in scope.	Consider referring to the 'life cycle' of the data processing to make it clear why these aspects are in scope.
		Does not say anything is out of scope. There are some aspects of UK GDPR not covered, eg Article 8 and Article 22. Presumably this is because they are out of scope, but this is not clear.	Make sure any aspects of UK GDPR that are out of scope are noted, providing reasons.
Territorial scope defined	Yes	**LOCS Certification Standard, Scope section, p.6** *"The LOCS:21 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 relate to the offering of legal services (even if for free) to data subjects situated in the United Kingdom."*	-

4. Object of certification/Target of Evaluation (ToE)			
Criteria sufficiently describe how the ToE (object of certification) should be defined by the controller/processor	Partially	**<u>LOCS Certification Standard, Scope section, Target of Evaluation, p.5</u>** *"An applicant for LOCS:21 accreditation will be required to document the processing activities being presented for certification in terms of the types of data being processed (e.g., special category data, biometric data, etc.), as well as the systems and processes used.* *The applicant will also be required to provide details of the following:* • *Location of processing* • *Sub-processors used* • *Internal governance structure* • *Existing relevant certifications"* The purpose of this section is to describe to the organisation being certified (applicant) how to define the processing operation(s) to be certified. Therefore this section requires more details on how to identify and define the processing operations subject to certification. There is no reference to organisations justifying any exclusions from the ToE.	Expand this section to set requirements for the applicant to clearly describe the processing to be certified, including to: • define the ToE in terms of data types, systems, and processes used; • define where the processing that is subject to evaluation starts and ends, including all interfaces with other interdependent processing operations; • justify ToE's exclusions and interfaces with interdependent processing; • identify and reflect special types of processing eg automated decision making, profiling, high risk processing; and • identify special category data involved in the processing
		The introduction refers to 'legal technology' and says that this is an important consideration for legal service providers. However this is not mentioned in the ToE section.	As considering the data protection compliance of 'legal technology' is an important part of the scheme it will be necessary for organisations to define the relevant systems which constitute 'legal technology' when applying for certification.
		Clarification required on 2nd paragraph: 'processes in scope will undertake activities….' As processes can't undertake activities it is unclear if this should actually refer to processors.	Amend wording to reflect the intention here.

Criteria guarantee that the ToE (and therefore resulting certification) will be understandable to intended audience incl. data subjects	No	Needs further expansion as per above to meet this requirement.	As above.
5. Criteria			
Criteria allow accreditation to ISO17065 standard (ie do not contradict any of the accreditation requirements and apply to processing operations contained within a product or service ***not*** a management system)	No	Criteria are very high level. To be compatible with ISO 17065 they need to set specific and auditable requirements for the processing of personal data within the context of legal client services. There is a large focus on policies and procedures both in the standard and the assessment criteria document. To be compatible with ISO 17065 and meet our requirements there needs to be a greater focus on the processing itself in the context of the legal client data file, with criteria written in terms of what compliance with UK GDPR looks like in practical terms.	Ensure criteria are largely focussed on the processing activity that is in scope. They should set specific, objective, and auditable requirements outlining what is the expected outcome/result based on its objective.
Criteria cover all the relevant UK GDPR responsibilities (below), procedures and processing defined by the scope and require technical and organisational measures guaranteeing protection in line with below.	Partially	The scope should set out which aspects of the UK GDPR apply/don't apply to the data processing activities; criteria should then outline the technical and organisational measures organisations must implement in order to comply with those responsibilities. Most aspects of UK GDPR are not covered in sufficient detail, and some aren't covered at all.	*See comments and recommendations below.*
i. principles of data processing (Art 5)	Partially	**LOCS Certification Standard** This is covered in the governance section and restates UK GDPR. Covering the principles at a high level in this section would be fine if there were more detailed criteria relating to each one elsewhere in the	Ensure there are detailed requirements in the standard that practically apply the data protection principles. You can see ICO guidance on principles the accountability framework (in particular the records management section) for more information.

		document, for example requirements for how organisations ensure accuracy of data on collection and throughout the lifecycle of the data. However that is not the case. There is also no reference to the accountability principle [Art 5(2)].	
ii. lawfulness of processing (Art 6-10)	Partially	**LOCS Certification Standard, 2.3** says that the organisation must 'indicate' the lawful basis it is relying on. Organisation go further than just indicating the basis. For example, they should have documented the basis for each of their processing activities, have checked the processing is necessary for the relevant purpose and be able to justify their decision.	Ensure requirements for lawfulness of processing fully reflect the legislation (including recitals) and ICO Lawful basis for processing guidance.
		2.3.1 refers to the 'lawful processing principles'. These are the lawful *bases* set out in the UK GDPR, not principles. Refers to Article 9 lawful basis but we refer to these as 'conditions for processing' as you cannot process special category data unless you can satisfy one of the conditions in Art 9(2) applies.	Use correct terminology when referring to lawful bases.
		2.3.1 restates UK GDPR and does not set any specific requirements for each of the lawful bases.	Set practical requirements relating to each of the lawful bases.
		Article 7 not covered re. conditions for consent.	Ensure Article 7 is covered when setting requirements for consent.
		Article 8 not covered. Presumably this is because it is out of scope as it relates to child's consent in relation to information society services. If that is the case, then this should be reflected in the Scope section.	Ensure any aspects of UK GDPR that are out of scope are reflected in the scope section of the standard and/or in guidance notes as appropriate.

iii. data subjects' rights (Art 12-23)	Partially	**<u>LOCS Certification Standard</u>** **2.10 Data subject rights**	-
		<u>Art 12 – transparent information, communication, and modalities DS to exercise their rights</u> – Not covered? Art 12(1) No reference to how information should be communicated, ie concise, transparent, intelligible, easily accessible form, using clear and plain language, etc. Art 12(3) DS rights sections refer to providing the information with undue delay but no reference to providing it within one month of receipt of request. Art 12(4)-(6) – not covered.	Ensure the obligations from Article 12 are reflected in the requirements for the relevant DS rights (or separately as appropriate).
		<u>Art 13 – right to be informed</u> – **2.10.1 Right to information** cross references **2.7 privacy notices - 2.7.1 DS privacy notice**, **2.7.2 Employee privacy notice**. Not certain if employee privacy notice is relevant as the scope relates to the processing for client legal file, not HR processing.	Consider if it is necessary to have requirements for employee privacy notice if HR processing not in scope.
		<u>Art 14 – information where data obtained from third parties</u> – appears to be incorporated into **2.7.1**. However, Art 14(4) not covered, and exceptions set out in Art 14(5) not referenced.	Check that all aspects of Article 14 are covered in **2.7.1**.
		<u>Art 15 – right of access</u> – **2.8.2** refers to DSAR register. 'DSAR' is not defined but presumably this means 'data subject access requests'. If so, this only refers to the right of access whereas **2.8.2**	Make sure title of section reflects the content or vice versa. Ensure that ALL data subject rights requests are logged and managed effectively. That is not to say there can't be

		says *"An organisation MUST maintain a register of all Data Subject Right Requests."* However, it then goes on to say *"An organisation MUST collect the following information for Subject Access Requests…"* There is then another section at **2.11.2** – Data Request Management. This also only refers to SARs (not DSARs), including staff awareness and so other requests are not given equal treatment.	additional requirements for tracking information requests if necessary.
		2.11.2 states that a SAR form must be completed. Organisations can provide such a form but cannot insist on individuals completing one to make a request for their information.	If the requirement to provide a form is retained add a note to explain organisations cannot insist on individuals using it.
		Art 15 - **2.10.2** restates UK GDPR.	Ensure criteria go further that restating UK GDPR by setting specific requirements relating to each of the rights. Make sure that all aspects of each right are covered.
		Art 16 – right to rectification – **2.10.3** restates UK GDPR but omits the right to have incomplete personal data completed by providing a supplementary statement.	
		Art 17 – right to erasure – **2.10.4** restates UK GDPR.	
		Art 18 – right to restriction – **2.10.5** restates UK	
		Art 19 – notification obligation – not covered.	
		Art 20 – right to data portability – **2.10.6** restates UK GDPR.	
		Art 21 – right to object – **2.10.7** restates UK GDPR.	

		Art 22 – automated decision making – rights relating to automated decision making not covered. Presumably this is because it is out of scope, but this isn't stated in the document.	Ensure any aspects of UK GDPR that are out of scope are stated in the scope section of the standard.
		Art 23 – restrictions – no reference to restrictions and exemptions.	Ensure the standard refers to restrictions and exemptions. These are set out in the DPA 18, Part 8, Schedule 2.
iv. general obligations of controllers and processors (Chapter IV – Art 24-31)	Partially	Art 24 – implementing, reviewing, and updating technical and organisational measures – Implementing technical and organisational measures should be covered by the requirements set by the scheme if they practically apply the legislation. Reviewing measures not explicitly covered. Section 3 covers 'Monitor & Review' and covers internal audit, management review and external audit, however it does not refer to reviewing the effectiveness of technical organisational measure in place. Neither does section 4 re. 'Continuous Improvement', although there is a requirement to carry out PEN testing. 2.9 is titled 'Technical & Organisational Measures', however this section only seems to refer to security measures	Ensure there is a requirement for organisations to carry out a review effectiveness of technical and organisational measures and update where necessary.
		Art 25 – DP by Design and default - see below	-
		Art 26 – joint controllers – **s.2.6.3** All aspects appear to be covered. **2.6.1** refers to a 'statement of adequacy' and 'adequacy checklist' but no requirements are set for what is deemed adequate. Also	**2.6.1** - amend language so as not to be confused with adequacy in the context of international transfers.

		using the term 'adequacy' is confusing as this is referred to in international transfers when organisations are covered by adequacy regulations.	Also consider what satisfactory due diligence would look like for controllers.
		Art 27 – Representatives of controllers/processors not established in the UK – Not covered	Ensure Article 27 is covered as certification is open to organisations outside the UK.
		Art 28 – Processor – **s.2.5** requires a supplier register of 3rd part suppliers processing PD and **s.2.5.1** requires a supplier risk assessment to be carried out. It says if any of the criteria listed are met the supplier 'should' be considered high risk. It seems like this should rather be a requirement. **2.6** talks about 'third party data transfer' and includes data sharing between controller-controller (**2.6.1**) and controller – processor (**2.6.2**). **2.6.2** – says a 'data protection agreement' (should this be processing agreement?) must be agreed. However it does not stipulate what the agreement should contain in line with Article 28. The guidance note refers to larger suppliers where there is no contract. To comply with Art 28 there needs to be a contract or other legal act that is binding on the processor.	**2.5.1** - Consider if the 'should' statement should rather be a requirement. **2.6.2** – a) consider wording of 'data protection agreement' – should it say data processing agreement'? b) ensure Art 28 is fully reflected including requirements for what must be in a processing agreement. c) consider the implications of the guidance note and whether such a situation would comply with UK GDPR.
		Art 29 – processing under authority of controller – No reference to processor only acting on instructions of controller.	Ensure Article 29 is covered. This could be incorporated into **s.2.6.2**.
		Art 30 – Records of processing activities – covered at **2.2.** Outlines what records must contain. However doesn't appear to cover all	Ensure requirements fully reflect Article 30.

		the information required by Art 30, eg name and contact details of controller, purposes of processing, description of categories of data subjects and categories of data. Also doesn't make the distinction between requirements for controllers [Art 30(1)] vs processors [Art 30(2)].	
		Art 31 – cooperation with the ICO – Not covered.	Ensure Article 31 is covered.
v. obligation of DP by design and default (Art 25)	No	This is not specifically mentioned in the standard.	Ensure data protection by design and default is covered in the standard in the context of the processing in scope.
vi. information governance / data protection management system	Partially	**LOCS Certification Standard** Section 1 – Governance. **1.1** Covers 'scope' – should this be in this section? Would this not be covered by the certification application process? **1.2** Responsibility and accountability – privacy council, DPO, ICO registration. **1.3** Principles – restates UK GPDR. **1.4** DP policy – refers to several other policies relating to information security. A DP policy can incorporate the information security policy but should be much broader – setting out an organisations approach to data protection. 'User' training covered in **section 4** – Continuous improvement but doesn't really cover staff data protection training in sufficient detail. All staff require data protection training with additional role specific training as necessary. There are a number of other references to 'users', eg 'user training' an 'user account policy', but not clear re users of what.	Ensure this section provides detailed requirements relating to leadership and oversight, policies & procedures, transparency of processing operations (not necessarily right to be informed), records of processing (unless covered separately), contracts (unless covered separately), staff training and awareness, internal audit and continual improvement and is aligned to our accountability framework. Make sure language is self-explanatory if not defined.

vii. technical and organisational measures to ensure appropriate level of security (Art 32)	Partially	**LOCS Certification Standard** **2.9. Technical & Organisational Measures** This section sets some security requirements. However some refer to policies/procedures rather than practical measures. For example, 2.9.1.2 *"An organisation MUST have a documented procedure for applying system patches and updates."* This section could go further to set expectations for best practice for legal firms. For example, are client files taken out of the office for court proceedings? What security measures would be expected? **2.12 Physical security**. This contains quite general statements that don't seem to add much to section 2.9. Would suggest these sections are merged.	Ensure criteria set specific and practical requirements for information security that relate to the processing in scope. There are some examples in the Records management and security section of the accountability framework as well. Consider merging **section 2.12** into **2.9** (bearing in mind the recommendation above about specificity of the requirements.)
viii. obligation to notify data breaches (Art 33-34)	Partially	**LOCS Certification Standard** Section **2.8** refers to 'Incident Registers' and **2.8.1** to 'Breach Register'. This sets requirements for logging breaches and action taken. **2.11.1** 'Data Breach Management' in the 'Incident Management' section talks about organisations having a breach reporting process and reporting 'material breaches' to the ICO. The note says that 'material breaches' are where it has the potential to impact the rights and freedoms of the DS. There is no mention of reporting breaches to data subjects as per Article 34.	Ensure all aspects of Articles 33 and 34 are covered as well as expectations around the management of data breaches and is in line with our guidance on personal data breaches.
ix. assessment of risks to rights and freedoms of individuals including	Partially	**LOCS Certification Standard, s.2.1, DPIA** Must have a template (published and available. Must 'provide a DPIA' – to who?	Ensure requirements for DPIAs go beyond the policy document and template and fully

completion of DPIA where required (Art 35(7)(d))		Should this rather say complete? – for all changes to internal processes or systems that involve a high risk to personal data. The ICO has also published a list of circumstances where a DPIA is required to be carried out. This is only required to be evidenced by having a DPIA document (LOCS2:21:A5 – DPIA Document). No consideration of wider aspects of carrying out a DPIA. Doesn't reflect all aspects of Article 35 or ICO guidance on DPIAs. No mention of consulting affected parties or publishing DPIA. No reference to Art 36 and requirement to consult ICO where risk cannot be mitigated to acceptable level. **1.4.4 Service Procurement Policy** requires a DPIA when procuring new services that process high risk data. **2.4** – requirement for a risk register outlining any risks to data protection.	reflect Article 35 and 36 and ICO guidance on DPIAs.
x. DPO (Art 37-39)	Partially	**LOCS Certification Standard** **1.2.2 Data Protection Officer** – Refers to determining whether a DPO is required, documenting the decision process (minor but should this refer to documenting the decision rather than the process?), appointing an alternative where no DPO required. Also refers to registering DPO details with ICO. **2.7.1 Data Subject Privacy Notice** section refers to publishing details of DPO or alternative representative. No reference to tasks and position of the DPO.	Ensure requirements are set that fully reflect Articles 37-39. Ensure wording is clear to reflect desired outcome, eg 'documenting the decision'.

xi. international transfers (Art 44-49)	Partially	**LOCS Certification Standard** 2.6 Third Party Data Transfer 2.6.4 Transfer outside the UK or EEA This section is very brief and doesn't fully reflect Articles 44-49 or ICO international transfers guidance. Ultimately 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 (Art 45 – 47), or one of a limited number of exceptions applies (article 49). These are mentioned at a very high level but there are no requirements set for each of the relevant articles, and there is no requirement to carry out a transfer risk assessment. The first point refers to 'EU and/or UK Adequacy List', however only UK law will apply here. There are provisions which permit the transfer of personal data from UK to the EEA and to any countries which, **as at 31 December 2020**, were covered by a European Commission 'adequacy decision'. So if the EU adequacy list changed after that date, then it wouldn't necessarily be covered by these provisions. Re. the guidance note about consent as an exception – not certain where the statement about "*should only be used in exceptional circumstances and temporarily"* originates from. Also consent is not the only exception. Might 'contract' [Art 49(1)(b) and (c)] sometimes be relevant?	Ensure requirements for making international transfers fully reflect Articles 44 – 49 and ICO international transfers guidance.
xii. Criteria for the purpose of demonstrating the existence of appropriate	N/A	*N/A – the scheme is not intended as a transfer mechanism.*	-

safeguards for transfer of personal data in the meaning of Article 42(2) where the certification is intended to act as transfer tool in itself.			
Each criterion should also have alongside it an explanation (if necessary), implementation guidance and how compliance can be demonstrated for each criterion. *The latter two would not be binding but would serve as an indicator to users of the scheme of how the criteria should be implemented and compliance demonstrated. How compliance will be tested will be considered fully as part of the accreditation process for certification bodies and the certification process for controllers and processors*	Partially	*[This is a requirement of EDPB guidelines para 67 and explained in the ICO's detailed certification guidance.]* There are some guidance notes that provide possibilities or further explanation as required. There is no implementation/ demonstration guidance. Some notes are actually setting requirements and should rather be included in the criteria. For example, the guidance note at **2.4** says, *"The Risk Register must be kept updated as new risks occur or mitigations actioned."*	Ensure guidance notes are merely explanatory and are not setting normative requirements. Consider the use of implementation/demonstration guidance.
The criteria should support the practical application of the UK GDPR to the identified processing operations (target of evaluation)	No	Currently too general and in some areas merely restates UK GDPR. Needs more detailed criteria focussed on the processing of personal data to maintain a client data file to result in practical application.	To support the practical application of UK GDPR, criteria must go beyond the legislation specifying requirements for the characteristics of what is being certified.
6. Overall opinion			
Appears on first inspection to cover all relevant sections of UK GDPR that relate to the scope, ie. principles, rights, lawful basis, data protection by design and default, requirement to assess risks to rights and freedoms of individuals	No	Not all aspects of UK GDPR that relate to the processing are covered as per comments above. The areas that are covered require more detail.	

Allows meaningful DP certification considering the nature, content, risk, and scope of processing	No	The purpose of UK GDPR certification is that it allows organisations to demonstrate compliance with the legislation. Whilst the concept of UK GPDR certification for Legal Firms is valid, at this stage the criteria do not go sufficiently beyond the legislation to result in meaningful certification, and in our opinion would not enable controllers/processors to demonstrate their compliance with UK GDPR.
7. Outcome		
Meets initial requirements and can proceed to full assessment	No	Unfortunately on this occasion we have determined that the criteria do not meet our initial requirements. Criteria should be expanded/amended in line with our comments and recommendations above. They can then be resubmitted for consideration against the requirements set out in this document.
Date reviewed	29/10/2021	**Name: Sarah Carr – Senior Case Officer**

From:	timhyman@2twenty4consulting.com
To:	certification
Subject:	RE: Information Commissioner"s Office: Outcome of full assessment of LOCS:22 Standard v9
Date:	12 January 2023 10:56:15
Attachments:	image001.jpg LOCS Certification Standard v10.1.docx Certification scheme criteria assessment form LOCS v9_v1.0 (AM comments).docx

External: This email originated outside the ICO.

Hi Sarah

Happy New Year and I hope you had a relaxing break.

Please find attached the updated LOCS:23 certification standard v10.1 and associated assessment form with comments.

Many thanks

Tim

From: timhyman@2twenty4consulting.com
To: certification
Subject: RE: Information Commissioner"s Office: Outcome of full assessment of LOCS:22 Standard v9
Date: 13 January 2023 10:29:01
Attachments: image001.jpg
LOCS Certification Standard v10.2.docx

External: This email originated outside the ICO.
Hi Sarah

Sorry to be a nuisance but I noticed a missing word in the InfoSec Policy text so have corrected in the attached version 10.2

Tim

From: certification <certification@ico.org.uk>
Sent: 12 January 2023 15:05
To: timhyman@2twenty4consulting.com
Cc: certification <certification@ico.org.uk>
Subject: RE: Information Commissioner's Office: Outcome of full assessment of LOCS:22 Standard v9

Hi Tim

Happy New Year to you too. I had a good break thanks – just playing catch-up now.

Thank you for submitting the revised version of the LOCS Standard. I hope you had a break over Christmas with all the work that's gone into that! We will review the documents and get back to you as soon as possible.

Kind regards,

Sarah

Logo

Sarah Carr
Senior Case Officer (Codes & Certification)
Regulatory Policy Projects
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6750 F. 01625524510 ico.org.uk
twitter.com/iconews Livechat
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

---

From: timhyman@2twenty4consulting.com <timhyman@2twenty4consulting.com>
Sent: 12 January 2023 10:55
To: certification <certification@ico.org.uk>
Subject: RE: Information Commissioner's Office: Outcome of full assessment of LOCS:22 Standard v9

External: This email originated outside the ICO.
Hi Sarah

Happy New Year and I hope you had a relaxing break.

Please find attached the updated LOCS:23 certification standard v10.1 and associated assessment form with comments.

Many thanks

Tim

LEGAL SERVICES OPERATIONAL PRIVACY CERTIFICATION SCHEME

January 2023

LOCS:23 STANDARD V10.2

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

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.

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

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, that in providing legal services carry out any of the Processing activities in 'Processing Activities in scope':

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

Data Controllers may use Data Processors and/or Sub-processors to assist with the general Processing of Client data. These may include:

- 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 alumni data (many Legal Service Providers keep contact databases of ex-employees and clients)
- 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

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

- 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 – Standard for Data Deletion.

  See Guidelines for Media Sanitization (nist.gov)

- NIST AES – Standard 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.

'ICO' means the Information Commissioners Office, the UK Data Protection Authority.

'Information Commissioner' The Information Commissioner is responsible for providing leadership and strategic direction to the Information Commissioner's Office and acting as Accounting Officer for the Information Commissioner's Office.

'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 separate controllers or processors and legally distinct from the exporting Organisation (receivers) located outside the UK.

'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.

'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.
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. See summary table in Appendix 3. 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. **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. **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. **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	N/A
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; 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 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. **8.1.2.2** The Organisation SHALL document the decision. **8.1.2.3** If a DPO is not required by legislation the Organisation SHALL either voluntarily appoint a DPO or appoint an alternative responsibility for Data Protection (see **NB 4**). **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. **8.1.2.5** If a DPO is appointed, they SHALL have specific responsibilities in line with Article 39 of the UK GDPR including: d. 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; e. 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; f. providing or overseeing awareness-raising and training of staff involved in Client File Processing operations; g. to provide advice when requested as regards the data protection impact assessment and monitor its performance; h. to cooperate with the ICO; i. 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**). **8.1.2.6** In addition, a DPO SHALL in line with Article 38: a. have expert knowledge of data protection law and practices; b. report to the highest level of the business; c. operate independently; 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. **NB 2.** **8.1.2.2** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13** **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	Chapter 4, Section 4 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. **8.1.3.2** If applicable, the Organisation SHALL register the DPO's details with the ICO. **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	N/A
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** – there must be a lawful basis for Processing Client Personal Data, and a necessity of processing for it to be lawful (apart from 'consent'). This is typically 'for the purposes of a contract' between Legal Service Provider and Client. 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. Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense. **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. **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. **NB 4**. Further ICO guidance regarding lawfulness, fairness and transparency can be found here
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**. **8.1.4.3** If a new purpose for processing personal data already collected is proposed an Organisation SHALL only go ahead if: a. the new purpose is compatible with the original purpose; b. you get the individual's specific consent for the new purpose; or 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. **8.1.4.4** If a new purpose for processing personal data already collected is proposed based on **8.1.4.3a** 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; b. the context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect; c. the nature of the personal data – eg is it particularly sensitive; d. the possible consequences for individuals of the new processing; and

	e. whether there are appropriate safeguards – e.g. encryption or pseudonymisation.
CONTROL APPLICATION GUIDANCE	**NB 5.** 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. **NB 6.** The following purposes will be considered 'compatible' as laid out in **8.1.4.3 (a)** a. archiving purposes in the public interest; b. scientific or historical research purposes; and c. statistical purposes. **NB 7.** 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. **NB 8**. 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 9.** Any surplus data provided by the Client should be deleted as laid out in **8.1.7**. **NB 10**. 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'). **8.1.4.7** The Organisation SHOULD provide a self-service mechanism for Data Subjects to assist maintenance with personal data. **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. **8.1.4.9** In order to ensure that records are not inaccurate or misleading, an Organisation SHALL: a. accurately record the information provided; b. accurately record the source of the information; c. take reasonable steps in the circumstances to ensure the accuracy of the information; and d. carefully consider any challenges to the accuracy of the information.
CONTROL APPLICATION GUIDANCE	**NB 11.** 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.

	NB 12. Data Subjects have the absolute right to have incorrect personal data rectified – see **8.2.4** **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**. **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. **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. **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: d. Record of Processing Activities (**8.3.3**); e. Data Retention Schedule (**8.1.7**); f. Personal Data Breach logs (**8.3.5**); g. Client Rights Response logs (**8.3.6**); h. Completed DPIAs (**8.3.2**); i. Third-party due diligence checklists (**8.4.3**); j. Third-party Processing Agreements (**8.4.4**); k. Transfer Impact Assessments (**8.4.6**); l. Privacy Notice (**8.2.2**); m. Training Records (**8.3.9**); n. Internal Audits (**8.5**). **NB 19**. Further ICO guidance regarding accountability can be found here
DATA PROCESSOR ALTERNATIVE CONTROL	Data Processors SHALL: a. act on the instructions of the controller,

	b. notify the controller if any of their instructions would lead to a breach of UK data protection laws, and c. assist the controller in meeting their data protection obligations. 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	Chapter 2 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: a. Data Protection principles b. The types of Client data processed and the purpose c. How data is collected d. Who data is shared with e. How long data is kept f. How data is protected g. Client File access h. Working remotely i. Sending Client documents securely j. Data classification k. Acceptable use of IT l. Removable devices **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: a. Access Control b. Encryption c. Asset Control d. Network Security e. Acceptable Use f. Password Management g. Incident Management h. Breach Notification i. Email Usage j. Clear Desk and Clear Screen k. Removable Media l. Patch Management

	m. Documents and Records Control n. Electronic destruction o. Remote working **8.1.5.3** The Organisation SHALL make the Data Protection and information security policies available to all employees. **8.1.5.4** The Organisation SHOULD audit employee awareness of the policies on a regular (at least annual) basis. **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** **NB 2.** The requirements of **8.1.5.2** are met if the ISO 27001:13 standards are in place.
DATA PROCESSOR ALTERNATIVE CONTROL	None – **8.1.5** applies equally to Data Processors
UK GDPR REFERENCE	Chapter 2 Article 5 (1) f
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. **8.1.6.2** The Organisation SHALL make the Business Continuity Plan available to all employees. **8.1.6.3** The Organisation SHALL regularly test the Business Continuity Plan and document results. **8.1.6.4** The Organisation SHOULD audit employee awareness of the plan. **8.1.6.5** The Business Continuity Plan SHALL include at least the following: a. A list of relevant contacts and contact details b. Detailed list of systems and data structures required to enable Client access to their data. c. Descriptions of disruption scenarios and recommended next step actions for each 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. **NB 2.** It is recommended that Information Security or Data Protection training carried out contains a reference to the Business Continuity Plan. **NB 3.** It is recommended that periodic reminder notices of

	the Business Continuity Plan are sent out to all employees. **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	Chapter 2 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. **8.1.7.2** The Organisation SHALL make the Retention & Destruction Policy available to all employees. **8.1.7.3** The Organisation SHOULD audit employee awareness of the policy. **8.1.7.4** The Organisation SHALL reference retention periods in the Record of Processing Activities, as laid out in **8.3.3.** **8.1.7.5** The Organisation SHALL allocate responsibility for destroying Client File records in line with the Data Retention and Destruction Policy. **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. **8.1.7.7** The Organisation SHALL implement regular diarised activities to ensure Personal Data is deleted in line with the Data Retention schedule. **8.1.7.8** The retention periods SHALL be further broken down into activity types such as 'Client due diligence data', 'matter data', 'Client contact data' etc. as each may necessitate different retention periods. **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.
CONTROL APPLICATION GUIDANCE	**NB 1.** The agreed Retention periods should be added to the ROPA (**8.3.3**). **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. **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)
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	Chapter 2 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.

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. **8.2.1.2** The Organisation SHALL when responding to a Data Subject follow the operational requirements as laid out in **8.3.6.** **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. **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. **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. **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. **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. **8.2.1.8** Information provided and any communication and any actions taken SHALL be provided free of charge. **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: 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. The Organisation SHALL document why they consider the request is manifestly unfounded or excessive.

	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. **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. **8.2.1.12** The Organisation may charge a reasonable fee when providing further copies of information under right of access. **8.2.1.13** 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. **8.2.1.14** If a self-service portal is unavailable documents SHALL be password protected before being returned by email.
CONTROL APPLICATION GUIDANCE	**NB 1.** 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. **NB 2.** 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. **NB 3.** Possible exemptions can be found in the DPA 2018 Schedule 2
DATA PROCESSOR ALTERNATIVE CONTROL	**8.2.1.1 – 8.2.1.12** do not apply to Data Processors Data Processors do not have to respond to Data Subject requests directly but will need to assist the Data Controller in applying Data Subject rights. See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Article 12
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: a. the identity and the contact details of the Organisation and, where applicable, of the Organisation's representative; b. the contact details of the Data Protection Officer if one is appointed; c. the purposes of the Processing for which the personal data are intended as well as the legal basis for the processing; d. where the Processing is based on legitimate interests, details of the legitimate interests pursued by the Organisation or by a third party; e. the recipients or categories of recipients of the Personal Data, if any; f. where applicable, that the Organisation intends to transfer Personal Data to a recipient in a third country or international Organisation and the means to obtain a copy of any safeguards where they have been made available. 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. 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; 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; j. the right to lodge a complaint with the Information Commissioner ; 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; 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. **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: a. the identity and the contact details of the Organisation and, where applicable, of the Organisation's representative; b. the contact details of the Data Protection Officer, or alternative; c. the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing; d. the categories of Personal Data concerned; e. the recipients or categories of recipients of the Personal Data, if any;

	f. where applicable, that the Organisation intends to transfer Personal Data to a recipient in a third country or international Organisation and the means to obtain a copy of any safeguards where they have been made available. 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.** **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). The website Privacy Notice and information provided in the Data Subject engagement process are examples of how this information can be provided. **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. **NB 3.** An Organisation should when providing privacy information to individuals, use a combination of techniques, such as: a. a layered approach for easy navigation; b. dashboards; c. just-in-time notices; d. icons; and e. mobile and smart device functionalities. **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: 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; 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; 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. **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. **NB 6.** Possible exemptions can be found in the DPA 2018 Schedule 2
DATA PROCESSOR ALTERNATIVE CONTROL	**8.2.2** Data Processors should assist Data Controllers. See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Section 1 Article 14-15
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. **8.2.3.2** When responding to the request, alongside any data that is provided, the Organisation SHALL also inform the Data Subject of: a. the purposes of the Processing. b. the categories of Personal Data concerned; 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; 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; 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; f. the right to lodge a complaint with the Information Commissioner (ICO); g. where the Personal Data are not collected from the Data Subject, any available information as to their source; 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. **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. **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. **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. **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. **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. **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. **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. **NB 3.** Exemptions can be found in the DPA 2018 Schedule 2.
DATA PROCESSOR ALTERNATIVE CONTROL	**8.2.3.1 – 8.2.3.7** do not apply to Data Processors See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Section 2 Article 15
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. **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. **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.** **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. **8.2.4.5** If asked, the Organisation SHALL inform the Data Subject which Third Parties have received the Personal Data. **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. **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. **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 See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Section 3 Article 16
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. **8.2.5.2** The Organisation SHALL erase Personal Data without undue delay where one of the circumstances in **NB 1** apply. **8.2.5.3** The Organisation SHALL erase Personal Data from all systems, including backup and archival systems. **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. **8.2.5.5** The Organisation SHALL inform the Data Subject about those recipients if the Data Subject requests it. **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. **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.**
CONTROL APPLICATION GUIDANCE	**NB 1**. This is not an absolute right and only applies in the following circumstances: a. the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; 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; 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); d. the Personal Data have been unlawfully processed; e. the Personal Data have to be erased for compliance with a legal obligation under domestic law; f. the Personal Data have been collected in relation to the offer of information society services referred to in Article 8(1). **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. **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.** This right shall not apply to the extent that Processing is necessary for: a. exercising the right of freedom of expression and information; 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; 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); 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 e. the establishment, exercise or defence of legal claims. **NB 5.** Exemptions can be found in the DPA 2018 Schedule 2
DATA PROCESSOR ALTERNATIVE CONTROL	**8.2.5.1 – 8.2.5.7** do not apply to Data Processors. See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Section 3 Article 17
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. **8.2.6.2** The Organisation SHALL restrict the Processing of data without undue delay where one of the circumstances in **NB 1** apply. **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. **8.2.6.4** The Organisation SHALL inform the Data Subject about those recipients if the Data Subject requests it. **8.2.6.5** The Organisation SHALL not process the restricted data in any way except to store it unless: a. they have the consent of the Data Subject; b. it is for the establishment, exercise or defence of legal claims; c. it is for the protection of the rights of another person (natural or legal); or d. it is for reasons of important public interest. **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. **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.** **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: 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; b. the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead; 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; 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. **NB 2.** Examples of how to restrict Processing include: • temporarily moving the data to another Processing system; • making the data unavailable to users; or • temporarily removing published data from a website. **NB 3.** The circumstances for when an Organisation should temporarily restrict processing include:

	• the individual has disputed the accuracy of the Personal Data and you are investigating this; or 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. **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. See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Section 3 Article 18
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. **8.2.7.2** Where the individual has provided data to the Organisation, and the Processing is: a. based on consent or contract; and b. is carried out by automated means, the Organisation SHALL, on request from the Data Subject: c. provide the data to the Data Subject in a structured, commonly used, and machine-readable format; and d. transmit those data without hinderance to another Organisation where technically feasible. **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**. **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. **NB 2.** The right to portability only applies to data provided by a Data Subject and only to data processed by automated means. **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. **NB 4.** Exemptions can be found in the DPA 2018 Schedule 2
DATA PROCESSOR	**8.2.7.1 – 8.2.7.4** do not apply to data Processors.

ALTERNATIVE CONTROL	See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Section 3 Article 20
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. **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 b. the Processing is necessary for the establishment, exercise or defence of legal claims. **8.2.8.3** Where this request is complied with, the Organisation SHALL no longer process the Personal Data. **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. **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.** **8.2.8.6** Processing SHALL be restricted whilst the objection is being considered. **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. **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. **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. See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Section 4 Article 21
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. **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**. **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. 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; 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 c. is based on the Data Subject's explicit consent. **8.2.9.4** If automated decision making is to be used due to one of the above exceptions then an Organisation SHALL: a. offer the right to obtain human intervention; b. enable the Data Subject to express his or her point of view; 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. See also **8.3.6.14** and **8.3.6.15.**
UK GDPR REFERENCE	Chapter 3 Section 4 Article 22
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** **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. **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.** **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. **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. **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. **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.** **8.3.1.7** The Organisation SHALL regularly assess and manage risks, including audit and review of risk assessments. **DEFAULT** **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. **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. **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 set all software security

	settings to the highest level of security by default. **8.3.1.12** An Organisation SHALL anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals. **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. **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. **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. **8.3.1.16** An Organisation SHALL offer strong privacy defaults, user-friendly options and controls, and respect user preferences. **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. **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 designers and manufacturers take data protection issues into account. **8.3.1.19** An Organisation SHALL use privacy-enhancing technologies (PETs) to assist it in complying with its data protection by design obligations. **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. **NB 2.** Where possible all 'default' settings on software applications that assist with the processing of Client File Data should have the strongest security settings.
DATA PROCESSOR ALTERNATIVE CONTROL	None – **8.3.1** applies equally to Data Processors. **8.3.1.17** applies to Data Processors in the context of engaging sub-processors.
UK GDPR REFERENCE	Chapter 4 Section 1 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. **8.3.2.2** An Organisation SHALL have a process for employees and Third Parties to report risks. **8.3.2.3** An Organisation SHALL record risks in a risk register that clearly differentiates information risks. **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. **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. **8.3.2.6** An Organisation SHALL provide a DPIA template for internal use. **8.3.2.7** The template SHALL be published and available to all department heads or others that may introduce process change. **8.3.2.8** A DPIA SHALL be completed in particular where the Client File requires: 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 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; **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: 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; b. the purposes and means of the intended Processing;

	c. the measures and safeguards provided to protect the rights and freedoms of Clients pursuant to this Regulation; d. where applicable, the contact details of the DPO; e. the data protection impact assessment provided for and; f. any other information requested by the Information Commissioner. **8.3.2.10** The Organisation SHALL seek the advice of the Data Protection Officer, where designated, when carrying out a DPIA. **8.3.2.11** A DPIA SHALL contain as a minimum: a. a systematic description of the Processing operations and the purposes of the Processing; b. an assessment of the necessity and proportionality of the Processing operations in relation to the purposes; c. an assessment of the risks to the rights and freedoms of Clients; d. the risk category of Personal Data; e. abnormal conditions and reasonably foreseeable situations that may lead to Personal Data breaches; f. the measures to address the risks, including safeguards. **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. **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. The Short Form DPIA is a basic assessment that includes the following: • What data categories will be processed? • Where will the data be located? • Where will the data be processed? • Who can access the data? • Will the data be shared? • How will the data be protected? • How long will the data be kept? 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 (oe equivalent) will assess any associated risks and determine whether a Long Form DPIA is initiated.

	The Long Form DPIA will be laid out as described in **8.3.2.10**. **NB 2.** The following process is recommended: a. The stakeholder proposing the process change or new solution initiates the Short Form DPIA and includes as much information as possible. 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. c. The DPO documents any potential risks and advises as to remediations indicating any remaining risks. d. The DPO provides the completed DPIA for senior management sign off e. The DPIA is reviewed at pre-determined intervals during the process change lifecycle. 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. **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. **NB 4.** An ICO DPIA template is available here **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. **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 – 8.3.2.13** do not apply to Data Processors. **8.3.2.15** A Data Processor SHALL have a process in place to identify, document, mitigate and manage information risks. **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	Chapter 4 Section 3 Article 35
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. **8.3.3.2** The Organisation SHALL maintain these records. **8.3.3.3** The ROPA SHALL contain: a. your Organisation's name and contact details, and where applicable, the Joint Controller, their representative and the DPO; b. the purposes of the Processing; c. a description of the categories of individuals and of Personal Data; d. the categories of recipients of Personal Data; e. details of transfers to third countries or international organisations, including a record of the transfer mechanism safeguards in place; f. retention schedules; and g. a description of the technical and organisational security measures in place. **8.3.3.4** The ROPA SHOULD also contain: a. The lawful basis for Processing; b. The IT systems used for Processing Client data; c. The geographical location of the data and/or the individuals Processing it; and **d.** A clear indication of the source of the data.
CONTROL APPLICATION GUIDANCE	**NB 1.** To prepare a ROPA it is recommended that you: a. Carry out an information audits using questionnaires for all business departments to find out what Personal Data the Organisation holds; b. review policies, procedures, contracts and agreements to address areas such as retention, security and data sharing. **NB 2.** It is also recommended that as part of an Accountability Framework, the ROPA links to the following: a. information required for privacy notices; b. records of any consent used; c. any controller-controller contracts d. any controller-processor contracts; e. Data Protection Impact Assessment reports; and f. records of Personal Data breaches g. Any documented Special Category Data processing h. Any documented Criminal data processing i. The Data Retention & Destruction Policy

<table>
<tr><td></td><td>
j. The Information Security Policy (8.1.5.2)

NB 3. Examples of categories of data include criminal offence, special category and children's data.

NB 4. 8.3.3.1 forms part of an Organisation's compliance with the principle of accountability described in 8.1.4.13

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)

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.
<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

Event preferences

Dietary Requirements</td><td>Provided by Client</td></tr>
<tr><td></td><td>Prospects</td><td>Contact Details</td><td>Event registration</td></tr>
</table>
</td></tr>
<tr><td>DATA PROCESSOR ALTERNATIVE CONTROL</td><td>
8.3.3.5 If an Organisation is a Data Processor, 8.3.3.3 is not applicable and instead its ROPA SHALL contain:
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;
b. Categories of Processing carried out on behalf of each controller;
c. details of transfers to third countries, including a record of the transfer mechanism safeguards in place;
d. a description of the technical and organisational security measures in place.
</td></tr>
<tr><td>UK GDPR REFERENCE</td><td>Chapter 4 Section 1 Article 30</td></tr>
<tr><td>AUDIT REFERENCE</td><td>LOCS:23:A19 – ROPA</td></tr>
</table>

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. **8.3.4.2** The Organisation SHALL not process Special Category Data unless one of the UK GDPR Article 9 conditions (see **NB 1.)**for Processing is met and documented. **8.3.4.3** The Organisation SHALL not process Criminal Offence Data unless it is either: a. under the control of official authority; or b. authorised by domestic law. This means meeting one of the conditions in Schedule 1 of the DPA 2018. **8.3.4.4** If an Organisation is relying on Article 9 conditions (b), (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 **8.3.4.5** If an Organisation is relying on Article 9 (b) as a lawful basis for processing, they SHALL have an 'appropriate policy document' (see link in **NB 3.)** **8.3.4.6** Where an Organisation relies on an appropriate policy document it SHALL during the relevant period (see NB— a. retain the appropriate policy document, b. review and (if appropriate) update it from time to time, and c. make it available to the Information Commissioner, on request, without charge.
CONTROL APPLICATION GUIDANCE	**NB 1.** The available **Article 6** lawful basis are: a. the data subject has given consent to the Processing of his or her Personal Data for one or more specific purposes ('consent'); 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'); c. Processing is necessary for compliance with a legal obligation to which the controller is subject ('legal obligation'); d. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person ('vital interest'); 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'); 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'). **NB 2.** The available **Article 9** Processing conditions are:

	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; 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; 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; 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; e. Processing relates to Personal Data which are manifestly made public by the Data Subject; f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; 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; 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; 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; 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. **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 **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 **NB 5.** The DPA 2018 defines 'relevant period' as used in **8.3.4.6** as a period which; 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. **NB 6**. The ICO have produced detailed guidance on the use of special category data here
CONTROL	**Consent** **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. **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. **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. **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. **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: a. Freely given and not a condition of service; b. Indicated by an affirmative action (no pre-ticked boxes); c. Not linked or combined with any other requirement for consent; d. Fully informed; e. Auditable; f. Separate for each Processing activity.
CONTROL APPLICATION GUIDANCE	**NB 7.** More advice and guidance on consent can be found here
CONTROL	**Contract** **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. **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: a. you have a contract with the Client and you need to process their Personal Data to comply with your obligations under the contract. 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). **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** **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. a. This does not apply to contractual obligations. b. The Processing must be necessary. If you can reasonably comply without Processing the personal data, this basis does not apply. c. You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning. 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** **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. **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: a. you need to process the Personal Data to protect someone's life. 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. 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. **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** **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. **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: a. 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or b. to perform a specific task in the public interest that is set out in law. 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. 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. 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. **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** **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. **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. **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**. **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. **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:

<table>
<tr><td></td><td>a. Identify a legitimate interest (purpose test);
b. Show that the processing is necessary to achieve it (necessity test); and
c. Balance it against the Client's interests, rights and freedoms (balancing test).

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:
a. Protect the interests of vulnerable groups such as people with learning disabilities or children;
b. Introduce safeguards to reduce any potentially negative impact;
c. Offer an opt-out;
d. Determine whether a DPIA is needed;
e. Document the decision and the assessment;
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.

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."

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

NB 17, The ICO have produced general guidance on the use of Legitimate Interest here

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
<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>
</table>

DATA PROCESSOR ALTERNATIVE CONTROL	**8.3.4** does not apply to Data Processors.
UK GDPR REFERENCE	Chapter 2 Article 6 Article 7 Article 9
AUDIT REFERENCE	LOCS:23:A20 – Lawful Processing

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. **8.3.5.2** An Organisation SHALL make all employees aware of the Personal Data Breach reporting process. **8.3.5.3** An Organisation SHALL report 'material' Personal Data Breaches, as defined in **NB 2**, to the ICO within 72 hours. **8.3.5.4** An Organisation SHALL report a high risk Personal Data Breach, as defined in **NB 3**, to the impacted Client without undue delay. **8.3.5.5** 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.). **8.3.5.6** An Organisation SHALL collect and record the following information for reported Personal Data Breaches: a. The date and time the breach was made known to the Organisation; b. The date and time the breach occurred; c. The name of the individual or supplier reporting the breach; d. The nature of the Personal Data Breach; e. The categories and approximate number of Data Subjects concerned; f. The categories and approximate number of data records concerned; g. Description of the likely consequences of the Personal Data Breach; 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. **8.3.5.7** 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. **8.3.5.8** If the ICO are informed of a Personal Data Breach, the following information SHALL be provided: a. a description of the nature of the Personal Data Breach including, where possible: b. the categories and approximate number of Clients concerned; c. the categories and approximate number of Personal Data records concerned; d. the name and contact details of the DPO or other

	contact point where more information can be obtained; 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. **8.3.5.9** If an affected Data Subject is informed of a Personal Data Breach, the following information SHALL be provided: g. the name and contact details of the Organisations DPO, or other contact point where more information can be obtained; h. a description of the likely consequences of the Personal Data Breach; 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; j. The fact that they have the right to raise a complaint to the ICO; k. Potential mitigation activities., and l. Useful links to 'next step' information or organisations. **8.3.5.10** 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** There are three types of Personal Data Breach. All must be reported immediately to the Data Protection Officer. 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). 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). 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). **NB 2. Reporting a 'material' breach to the ICO** 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. **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. **NB 4. Reporting a Personal Data Breach to the Data Subject** 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.** The communication to the data subject referred to in **NB 4**.is not required if any of the following conditions are met: 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; 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; c. it would involve disproportionate effort. **NB 6. Example Breach Reporting Process** a. All personnel must report a Personal Data Breach to the designated person immediately they become aware of the Personal Data Breach. 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). c. The DPO will confirm receipt of the report and log in the Personal Data Breach Register. d. The DPO will determine whether the Personal Data Breach needs to be reported to the Privacy Council and/or the ICO. e. The DPO will determine whether the Personal Data Breach is reportable to the Client(s) impacted. f. The DPO will make reports to d and e. **NB 7. Reporting a 'material' Personal Data Breach to the ICO - examples** 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. An example of a non-reportable breach – A memory stick containing multiple Client's email addresses has been lost. The memory stick is encrypted. **NB 8. Reporting a 'material' Personal Data Breach to the Data Subject - examples** 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 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**, **8.3.5.8** and **8.3.5.9** do not apply to Data Processors. **8.3.5.11** 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. **8.3.5.12** A Data Processor SHALL assist a Data Controller in complying with its own Personal Data Breach reporting obligations.
UK GDPR REFERENCE	Chapter 4 Section 2 Articles 33 - 34
AUDIT REFERENCE	LOCS:23:A21 – 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. **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. **8.3.6.3** The Organisation SHALL provide a self-service mechanism for Data Subjects to exercise their data protection rights. **8.3.6.4** The mechanism SHALL enable the Data Subject to submit a request electronically, verbally or in writing. **8.3.6.5** An Organisation SHALL make all employees aware of the Data Subject Rights Request Process. **8.3.6.6** An Organisation SHALL follow all requirements for a request as laid out in **8.2.1.** **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. **8.3.6.8** An Organisation SHALL maintain a register of all Data Subject Rights Requests. **8.3.6.9** The Register SHALL record the following information for Data Subject Rights Requests: a. Date of request b. Type of request c. Name d. Contact details e. Data requested f. Identity confirmed (where necessary) g. Actions taken h. Date concluded **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. **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.** **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**. **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. **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. **NB 3. The following is an example of a Data Subject Response Process** a. Any requests received by staff to be forwarded to the Data Protection Officer. b. DPO to log request in Data Subject Right Request Register and confirm identity of requestor. c. DPO to respond to requestor confirming the response to the request is underway. d. DPO to consider whether the request should be processed in light of any exemptions. e. DPO to instruct IT with search criteria including systems, time periods and search terms. f. IT to provide results to DPO g. DPO to redact other non-requestor Personal Data. h. If particularly sensitive DPO may submit his decision for approval by the Privacy Council. i. DPO to log the decision of Privacy Council in the Register. j. DPO is to share information with the requestor using secure method (e.g., encrypted memory stick or passworded zip file). **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 – 8.3.6.12** do not apply to Data Processors. **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. **8.3.6.15** The Data Processor SHALL assist the Data Controller with meeting its obligation to comply with those rights.
UK GDPR REFERENCE	Chapter 3 Section 3 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 that involve Personal Data processing in a Systems Map:
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: a. how the systems interact b. data flow c. type of data present d. system owner e. on/off premises 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. **8.3.7.3** An Organisation SHALL apply security patches immediately when they become available. **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. **NB 3.** The requirements of **8.3.7.2 – 8.3.7.4** are met if either the ISO 27001:13 or Cyber Essentials standards are in place.
CONTROL	**8.3.7.5** An Organisation SHALL have a backup and restore process in place for all Client data. **8.3.7.6** An Organisation SHALL encrypt at rest all backup data. **8.3.7.7** An Organisation SHALL test the restore function at least weekly. **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).** **NB 5.** The requirements of **8.3.7.5 – 8.3.7.8** are met if either the ISO 27001:13 or Cyber Essentials standards are in place.

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 appropriate staff training. **8.3.7.10** At a minimum, encryption SHALL be to NIST Advanced Encryption Standard **8.3.7.11** An Organisation SHALL enable the encryption of data on removable devices that process Client File data. **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 6.** 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. **NB 7**. Link to NIST AES in normative references above. **NB 8.** 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 9.** Good network security helps prevent unwanted external access and reduces risks such as data theft and ransomware attacks. Examples of protective technologies include: a. Firewalls b. Anti-Virus/Malware c. Network Access Security d. Penetration Tests e. Multi Factor Authentication **NB 10.** The requirements of **8.3.7.13** are met if either the ISO 27001:13 or Cyber Essentials standards are in place.
CONTROL	**8.3.7.14** An Organisation SHALL implement an external vulnerability scan at least once a year. **8.3.7.15** An Organisation SHALL implement an internal vulnerability scan at least once a year.
CONTROL APPLICATION GUIDANCE	**NB 11.** 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. **NB 12.** An internal scan will expose any risks present on the internal network. **NB 13.** The requirements of **8.3.7.14 – 8.3.7.15** are met if either the ISO 27001:13 or Cyber Essentials standards are in place.
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 14.** The biggest risk to breach of Client File data is human error. Solutions that can help reduce the risk of accidental disclosure include: a. Data Leakage Protection b. Threat Detection

	c. Mobile Device Management d. Training
CONTROL	**8.3.7.17** An Organisation SHALL use anonymisation, where possible, to reduce the amount of personal data being processed. **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 15.** 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. **NB 16.** 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. **NB 17**. 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. **NB 18**. Applying **8.3.7.15** and/or **8.3.7.16** will assist with compliance with the data minimisation principle (**8.1.4.5**) **NB 19**. ICO guidance on security can be found here
DATA PROCESSOR ALTERNATIVE CONTROL	None – **8.3.7** Applies equally to Data Processors.
UK GDPR REFERENCE	Chapter 2 Article 5 (f)
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 to them. It is recommended that 'Open' systems are avoided. **NB 2.** The requirements of **8.3.8.1** are met if either the ISO 27001:13 or Cyber Essentials standards are in place.
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: a. Device Name

	b. Device Type c. Serial No d. MAC address e. Primary Device User **NB 4.** The requirements of **8.3.8.2** are met if the ISO 27001:13 standards is in place.
CONTROL	**8.3.8.3** An Organisation SHALL delete electronic Client File data to a minimum of the NIST 800-88 standard prior to disposing of electronic equipment in line with parameters stated in the Retention & Destruction Policy (**8.1.7**)
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. Electronic data – this should be deleted/purged to NIST 800-88 standards. It is recommended that IT confirm the disposal.
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.** **8.3.8.5** When using a third-party service, an Organisation SHALL obtain a certificate of disposal.
CONTROL APPLICATION GUIDANCE	**NB 6.** 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. **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 7.** It is recommended that spot checks are carried out to confirm compliance. **NB 8.** The requirements of **8.3.8.6 – 8.3.8.7** are met if the ISO 27001:13 standard is in place.
CONTROL	**8.3.8.8** An Organisation SHALL protect paper documents and files.
CONTROL APPLICATION GUIDANCE	**NB 9.** 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 **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. **8.3.8.10** An Organisation SHALL log Client File data leaving and returning to site. **8.3.8.11** An Organisation SHALL implement an authorisation process for removing Client File data from site.
CONTROL APPLICATION GUIDANCE	**NB 10.** 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.

	a. Best practice guidance may include: b. Not leaving Client File data unattended c. Reading Client File data in public d. Printing Client File data at home e. Returning Client File data to the office f. Secure disposal of Client File data
DATA PROCESSOR ALTERNATIVE CONTROL	None – **8.3.8** applies equally to Data Processors.
UK GDPR REFERENCE	Chapter 2 Article 5 (f)
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. **8.3.9.2** The Data Protection Training where electronic SHALL include a knowledge test with a minimum of 80% pass mark. **8.3.9.3** The Data Protection Training Programme SHALL include an auditable record of training delivered and attended. **8.3.9.4** The Organisation SHALL keep training records which SHALL be monitored to ensure all staff receive and complete Data Protection training. **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. **8.3.9.6** The Data Protection training SHALL be delivered at regular intervals (at least annually). **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. **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, **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. It is recommended that the Data Protection training covers at least the following: a. Definition of Personal Data b. Core areas of Client data Processing c. Sharing Client data with others d. What to do when there is a Personal Data Breach

	e. What to do when I receive a rights request from a Client f. Working Remotely g. Disposing of Client data h. The importance of providing privacy information to Data Subjects and when to do so. i. Specific modules for front-line staff **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	Chapter 4 Section 4 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. **8.4.1.2** The Organisation SHALL maintain these records.
CONTROL APPLICATION GUIDANCE	**NB 1.** These must be recorded in a Supplier Register. It may be useful to link these back to the ROPA. Suppliers may include (but are not limited to): a. Data Hosting b. External Legal Services c. Barristers d. Translation services e. Transcription services f. Financial Services g. Off-site paper file storage **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. See also **8.4.4.3** and **8.4.4.4.**
UK GDPR REFERENCE	N/A
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. **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 in the performance of the Commissioner's tasks. **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** '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; where the obligations of such Processing are determined by law, the controller or the specific criteria for its nomination may be provided for by law. For example, a Data Controller will determine: a. how to collect the Personal Data in the first place and the legal basis for doing so; b. which items of Personal Data to collect, i.e. the content of the data; c. the purpose or purposes for which the data are to be used; d. which individuals to collect data about; e. whether to disclose the data, and if so, to whom; f. whether subject access and other individuals' rights apply i.e. the application of exemptions; and g. how long to retain the data or whether to make non-routine amendments to the data. **NB 2. The Data Processor** 'Data Processor' means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller. For example, a Data Processor can determine: a. what information technology (IT) systems or other methods to use to collect Personal Data; b. how to store the Personal Data; c. the detail of the security surrounding the Personal Data; d. the means used to transfer the Personal Data from one Organisation to another; e. the means used to retrieve Personal Data about certain individuals; f. the method for ensuring adherence to a retention schedule; g. the means used to delete or dispose of the data. **NB 3. The Joint Controller** 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. **NB 4. Examples** 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. 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. **NB 5.** More detailed guidance on determining whether an Organisation is a controller/processor/joint controller can be found here: 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. See NB 2. for Data Processor definition. See also **8.4.4.3** and **8.4.4.4.**
UK GDPR REFERENCE	Chapter 4 Section 1 Article 24, Article 26, Article 28, 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. **8.4.3.2** The Organisation SHALL include the following in a documented due diligence check as a minimum: a. Where does Processing take place? b. Do they have a DPO (or equivalent Data Protection lead)? c. Do they have a Breach Reporting Process? d. What technical and Organisational measures are deployed? e. Where (in terms of geography) backup and development data will be located. f. Any relevant Technical & Organisational security measures in place. g. Do standard contract terms include data protection provisions? h. Do they maintain Data Processing Records? i. Will Personal Data be deleted or returned upon termination of contract at no extra cost? j. Do they offer full transparency of data transfer to other parties/destinations? 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? m. What is the Data Processor's data protection risk assessment process? **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.

	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. 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)** **8.4.4.1** Where a Data Processor is being engaged, a Data Processing Agreement (DPA) SHALL be agreed by both parties. **8.4.4.2** The Data Processing Agreement SHALL include clauses to ensure the Third Party: 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; 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; d. does not engage with another processor without prior specific or general written authorisation of the controller; 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; f. assists the controller in responding to requests from individuals to exercise their rights where applicable; 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; 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; 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; j. maintain a Record of Processing Activities as laid out in **8.3.3.5.** k. report Personal Data Breaches to the Controller within 24 hours of being made aware. **Processor to Processor (P-P)** **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 **8.4.4.4** Where a Data Processor has engaged another Data Processor as a sub-processor, the Data Processing Agreement between the two Processors SHALL include the same clauses and obligations as laid out in 8.4.4.2. **8.4.4.5** 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. **8.4.4.6** When a Data Processor engages another Processor it SHALL provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of UK GDPR.
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.
UK GDPR REFERENCE	Chapter 4 Section 1 Article 28 Article 29
DATA PROCESSOR ALTERNATIVE CONTROL	Data Processor controls indicated in **8.4.4.3 to 8.4.4.6**
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. **8.4.5.2** The Data Sharing Agreement SHALL include: a. The identity of the Data Controllers; b. The purpose of data sharing, including specific aims and why the data sharing is necessary; c. All Organisations involved in the data sharing, including contact details for key personnel and the DPO (or alternative); d. Which data items will be shared; e. The lawful basis for sharing data; f. Relevant conditions for Processing if the data being shared contains Special Category Data or criminal offence data. **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. **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. **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. **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. **NB 3.** **8.4.5.1** forms part of an Organisation's compliance with the principle of accountability described in **8.1.4.13** **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	N/A
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. **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). **8.4.6.3** The TRA SHALL comprise of the following: a. Location of Data Importer b. Proposed Lawful Transfer Mechanism (BCR/SCC/Derogation) c. What are the specific circumstances of the restricted transfer? d. What is the level of risk to people in the personal information you are transferring? 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 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); 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); d. the transfer is necessary for important reasons of public interest; 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) 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.; 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. 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 **NB 2.** 'Occasional Use' means that the restricted transfer may happen more than once but not regularly.

	NB 3. The legitimate interest exception is only for truly exceptional circumstances and where no other accepted safeguards are available. **NB 4**. The ICO have provided a TRA tool here **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. **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. **8.4.6.7** A Data Processor SHALL gain authorisation from the Data Controller before carrying out an international transfer. **8.4.6.8** If the Data Controller authorises an international transfer, **8.4.6** SHALL apply to the Data Processor. See also **8.4.**4
UK GDPR REFERENCE	Chapter 5 Articles 44-49
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. **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	Chapter 4 Section 1 Articles 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. **8.5.1.2** The internal audit process SHALL include a Control Audit Schedule. **8.5.1.3** The Audit SHALL include all areas indicated by LOCS:23 Audit References in this LOCS:23 Standard. **8.5.1.4** The Organisation SHALL produce an annual Audit Report. **8.5.1.5** The Audit Report SHALL be reviewed by the Privacy Council and at Management Review meetings. **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: a. Control Audit Frequency b. Control Owner c. Audit Sign Off **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. **NB 3. Example Process** a) Diarise annual audit meetings with key business stakeholders b) Design Internal Review Checklist (see appendix 4) c) Complete Internal Review Checklist d) Complete Review Report e) File Checklist and Report f) Report any outstanding risks to Senor Management. **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	N/A
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 review and document their findings and recommendations. **8.5.2.2** An Organisation SHALL update Data Protection Measures where necessary in line with audit findings. **8.5.2.3** An Organisation that is a Data Controller SHALL include the following Audit areas: **a. Accountability** 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: I. Policies (8.1) II. ROPA (8.3.3) III. Breach Register (8.3.5.5) IV. Data Subject Request Register (8.3.6.8) V. 3rd Party Supplier Register (8.4.1) VI. Awareness Training (8.3.9) **b. Privacy by Design** 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: I. DPIA (8.3.2) II. Default Privacy (8.3.1) **c. Privacy Notices** 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: I. Privacy Notices/Privacy information (8.2.2) II. Business Processing Privacy Notice (8.2.2) **d. Storage Limitation** This review area focuses on the data minimisation principle. The Organisation should ensure that existing policies and schedules are effective, up to date and periodic spot checks that each business area is actively meeting requirements. Key documentation to be audited are: I. Retention Schedule (8.1.7.6) II. Retention Policy (8.1.7)

	e. Data Sharing 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: I. Transfer Risk Assessment (TRA) (8.4.6.1) II. Procurement Due Diligence (8.4.3.2) III. Controller to Controller sharing agreements (8.4.5) IV. Controller to Processor sharing agreements (8.4.4) V. Processor to Processor sharing agreements (8.4.4) **f. Security** 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. I. New technology (8.3.7) II. Access control rights (8.3.1) III. Client data sharing practices (8.3.7) IV. Use of memory sticks (8.3.7) V. Locking of Filing Cabinets (8.3.8.7) VI. Vulnerability Scanning (8.3.7) **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. A Data Processor SHALL audit that all areas are consistent with any contracted agreement with a Data Controller and in particular that (a) III, (a) IV, (b) I and (e) I have capacity to assist a Data Controller.
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**).
DATA PROCESSOR ALTERNATIVE CONTROL	Partially applies - see **8.5.2.4**
UK GDPR REFERENCE	Chapter 4 Section 1 Article 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 4
ORGANISATION GOVERNANCE	GOVERNANCE	LOCS:23:C2	DPO decision	**SHALL**	Articles 37-39
ORGANISATION GOVERNANCE	GOVERNANCE	LOCS:23:C3	Registration	**SHALL**	Article 4
WORKING ON FILE	GOVERNANCE	LOCS:23:C4	Principles	**SHALL**	Article 5
WORKING ON FILE	GOVERNANCE	LOCS:23:C5	Data Protection and Information Security Policies	**SHALL**	Article 4
WORKING ON FILE	GOVERNANCE	LOCS:23:C6	Business Continuity Policy	**SHALL**	Article 5
CLOSING FILE (ARCHIVING)	GOVERNANCE	LOCS:23:C7	Data retention & Destruction Policy	**SHALL**	Article 5
WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C8	Transparency & Communication	**SHALL**	Article 12
WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C9	Right to Information	**SHALL**	Article 12
WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C10	Right to Access	**SHALL**	Article 15
WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C11	Right to Rectification	**SHALL**	Article 16
WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C12	Right to Erasure	**SHALL**	Article 17
WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C13	Right to Restrict Processing	**SHALL**	Article 18
WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C14	Right to Portability	**SHALL**	Article 20
WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C15	Right to Object	**SHALL**	Article 21

WORKING ON FILE – CLIENT ENGAGEMENT	CLIENT RIGHTS	LOCS:23:C16	Automated Decision Making	**SHALL**	Article 22
FILE GOVERNANCE	OPERATIONAL PRIVACY	LOCS:23:C17	Default Privacy	**SHALL**	Article 25
FILE GOVERNANCE	OPERATIONAL PRIVACY	LOCS:23:C18	DPIA	**SHALL**	Article 35
FILE GOVERNANCE	OPERATIONAL PRIVACY	LOCS:23:C19	ROPA	**SHALL**	Article 30
WORKING ON FILE	OPERATIONAL PRIVACY	LOCS:23:C20	Lawful Processing	**SHALL**	Articles 4.5,6,7 9, 10, 13, 14. 17, 28, 35
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**	Articles 16-22
FILE GOVERNANCE	OPERATIONAL PRIVACY	LOCS:23:C23	Technical Security Measures	**SHALL**	Article 32
FILE GOVERNANCE	OPERATIONAL PRIVACY	LOCS:23:C24	Organisational Security Measures	**SHALL**	Article 32
ORGANISATION GOVERNANCE	OPERATIONAL PRIVACY	LOCS:23:C25	Training	**SHALL**	Article 39
WORKING ON FILE – 3rd PARTIES	THIRD PARTY SERVICE PROVIDERS & DATA SHARING	LOCS:23:C26	Supplier Register	**SHALL**	Article 4
WORKING ON FILE – 3rd PARTIES	THIRD PARTY SERVICE PROVIDERS & DATA SHARING	LOCS:23:C27	Supplier Status	**SHALL**	Articles 24, 28, 29
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**	Articles 24, 28, 29
WORKING ON FILE – 3rd PARTIES	THIRD PARTY SERVICE PROVIDERS & DATA SHARING	LOCS:23:C30	C-C Data Sharing	**SHALL**	Articles 4 and 26
WORKING ON FILE – 3rd PARTIES	THIRD PARTY SERVICE PROVIDERS & DATA SHARING	LOCS:23:C31	Cross Border Data Transfer	**SHALL**	Articles 44-49
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 4
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	LOCS:23:C1 LOCS:23:C3 LOCS:23:C5 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:C4 LOCS:23:C6 LOCS:23:C7	Article 55	N/A
Article 6	LOCS:23:C19 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:C19	Article 59	N/A
Article 10	LOCS:23:C19 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	Article 65	N/A
Article 16	LOCS:23:C11	Article 67	N/A
Article 17	LOCS:23:C12	Article 68	N/A
Article 18	LOCS:23:C13	Article 69	N/A
Article 19	LOCS:23:C10 – C13	Article 70	N/A
Article 20	LOCS:23:C14	Article 71	N/A
Article 21	LOCS:23:C15	Article 72	N/A
Article 22	LOCS:23:C16	Article 73	N/A
Article 23	LOCS:23:C9 – C16	Article 74	N/A
Article 24	LOCS:23:C27	Article 75	N/A

Article 25	LOCS:23:C17	Article 76	N/A
Article 26	LOCS:23:C27	Article 77	LOCS:23:C8
Article 27	LOCS:23:C32	Article 78	N/A
Article 28	LOCS:23:C27	Article 79	LOCS:23:C8
Article 29	LOCS:23:C27	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 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	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:C29 LOCS:23:C30 LOCS:23:C31	Article 95	N/A
Article 45	LOCS:23:C29 LOCS:23:C30 LOCS:23:C31	Article 96	N/A
Article 46	LOCS:23:C29 LOCS:23:C30 LOCS:23:C31	Article 97	N/A
Article 47	LOCS:23:C29 LOCS:23:C30 LOCS:23:C31	Article 98	N/A
Article 48	N/A	Article 99	N/A
Article 49	LOCS:23:C30		
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	partially applies to Data Processors
LOCS:23:C10– Right of access	does not apply to Data Processors
LOCS:23:C11– Right of Rectification	does not apply to Data Processors
LOCS:23:C12– Right of Erasure	does not apply to Data Processors
LOCS:23:C13– Right to Restriction of Processing	does not apply to Data Processors
LOCS:23:C14 – Right to Portability	does not apply to Data Processors
LOCS:23:C15 – Right to Object	does not apply to Data Processors
LOCS:23:C16 – Automated Decision Making	does not apply to Data Processors
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		

2TWENTY4 CONSULTING
DATA PROTECTION SERVICES

YOUR DATA PROTECTED

www.2twenty4consulting.com
info@2twenty4consulting.com

www.locs23.com

From:	certification
To:	timhyman@2twenty4consulting.com
Subject:	The Information Commissioner"s Office: Review of revised LOCS:23 v10.2
Date:	23 February 2023 16:21:00
Attachments:	image001.jpg Certification scheme criteria assessment form v2.0 re LOCS v10.2.docx

Dear Tim
We have now had the opportunity to complete a review of the revised LOCS Standard submitted on 13 January 2022:

- **Legal Services Operational Privacy Certification Scheme: LOCS:23 Standard v10.2**

In response, please find attached the revised version (v2.0) of the assessment document.

We appreciate the work that has gone into amending the documents, however there are some further revisions needed.

We have indicated in the last column whether the required actions are complete, partially, or not complete, and have made comments in blue on the assessment document, highlighting where we believe that further amendments are necessary.

We have updated section P - Overall evaluation of criteria, as well as the second column indicating whether the requirement is met, to reflect the current position.

Please, as previously:

- Save all tracked changes in v10.2 and create a new version;
- Review our comments and implement any required actions;
- Complete the last column on the assessment form, detailing what action has been taken in line with ICO comments;

Once you have done this you should carry out an editorial check and return the amended scheme document with tracked changes, along with the completed assessment form.
We will then be able to consider whether the revised document fully meets our requirements.
Please let me know if you would like to organise a call to discuss any matters arising once you have had an opportunity to review the attached document.
Kind regards,
Sarah

Logo

Sarah Carr
Senior Case Officer (Codes & Certification)
Regulatory Policy Projects
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6750 F. 01625524510 ico.org.uk

twitter.com/iconews Livechat
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

Certification Scheme Criteria Assessment

Scheme details

Certification scheme name	Legal Services Operational Privacy Certification Scheme
Submitted version number	v9
Organisation	2Twenty4 Consulting
Date submitted	12/10/2022
Resubmitted	v10.2 - 13/01/2023

Publication of the criteria of certification

Can the criteria be published as submitted to the ICO?	Yes
Note: When the criteria of certification have been drafted by a scheme owner, the ICO needs to make sure that the version that will be made public has been submitted.	
Can the criteria of certification be made public free of charge?	Yes
Is the usage of criteria subject to trademarks, patents or copyrights[1]?	Yes
[If yes – please ensure that the conditions set up by the scheme owner do not interfere with UK GDPR requirements, EDPB guidelines or ISO 17065 plus ICO additional accreditation requirements for certification bodies]	

Type of certification mechanism

National certification criteria	Yes
Note: The ICO is not in a position to assess schemes intended as EU DP Seal.	
Have the certification criteria been sent to more than one Member State?	No
[If yes, please provide information about the criteria that has been submitted and list the Supervisory Authorities that are interested in approving the certification criteria.]	

Date assessment commenced	14/11/2022
V10.2	8/2/2023

[1] When the criteria of certification are subject to trademarks, patents or copyrights, the ICO needs to make sure that the conditions set up by the scheme owner do not interfere with UK GDPR requirements or EDPB guidelines.

Requirement	Yes No Partially	Criteria doc Section	Comments	Required action	Action taken
A. Scope					
1. Is the scope for which the DP criteria shall be used clearly described? [Annex 2 ref. 2a.]	Partially	2.0	**Section 2** covers the scope of the scheme including: 2.1 Scope of Certification Scheme Standard 2.2 Types of Organisations in Scope 2.3 Processing Activities in Scope 2.4 Target of Evaluation 2.5 Territorial Scope 2.6 UK GDPR areas out of scope 2.7 Processing areas out of scope. It was felt that for the most part the scope was clearly described other than where we have commented below.	-	-
		2.0	This states that *"Client data including any Personal Data will be kept as a single electronic record of the Client engagement known as the 'Client File'."* However, it was noted that while no doubt there will be an electronic record of the client which contains their personal data, this will not be the only storage area, for example there may be emails, both internal and external. There may also be hardcopy documents. For example, wills, court orders, marriage/birth/death certificates, share certificates, identification documents and other documents that can still be in paper form.	1. **2.0** - Ensure the description of the client file in the scope section matches the definition in **section 4**, providing for the fact the information in the client file may be held in multiple locations and consist of both physical and electronic records.	Scope amended to reflect definition of client file COMPLETE

			This is confirmed by the definition of the 'Client File' in **section 4** which states it is *"The physical or electronic collection of Client data relating to services afforded by a Legal Service Provider."*		
		2.2	Colleagues with knowledge/experience of the legal sector questioned the specific inclusion of actuaries in the list of organisations in scope at **2.2**. The first list appears to be for legal services providers (ie an organisation offering legal services to clients); however this is not explicitly stated – more implied by the last bullet point which says, "other providers of legal services". As actuaries don't provide legal services it was felt that they shouldn't be included in this list and would likely be covered by the second list under 'external consultants' or 'service providers'. There is also a question about whether the types of organisations in the second list would always be categorised as data processors.	2. Clarify the purpose of each list. For example, is the first list for types of legal service provider and the second for other types of organisations assisting with the processing? In which case, consider if the organisations in the second list will always be processors (eg, *"3rd Party Legal Service Providers*") and amend the heading if necessary. If the first list is for types of legal service providers, then remove actuaries from the list.	Both lists clarified to Data Controllers and Processors/sub-processors PARTIALLY Now **2.3**. This specifies the types of organisations in scope of the standard. The first list now only specifies types of controllers who can apply for certification. The second list says, "Data Controllers may use Data Processors and/or Sub-processors to assist with the general Processing of Client data. These may include…", which makes it sound like these organisations (processors/sub-processors) are not necessarily in scope of the scheme. Also, a sub-processor is a processor sub-contracted by the processor not the controller. It may be better to keep the original wording at the beginning of the section, then follow it with sub-headings for

					controllers in scope (1st list) and processors in scope (2nd list). Actuaries removed COMPLETE
2. Is the scope meaningful to its addressed audience and not misleading? [Annex 2 ref. 2b.]	Partially	2.0	It was felt that for the most part the scope of the scheme is clearly described and will be understandable to multiple audiences. However, to fully meet this requirement the comments in this section relating to the scope must be addressed.	*See required actions in this section.*	Recommendations actioned PARTIALLY Some minor amends required.
3. Does the scope reflect all relevant aspects of processing operations (including relevant phases of processing and whole-life-cycle of data)? [Annex 2 ref. 2c.]	Yes	2.1	This outlines the types of activities connected with maintaining the client file, eg initial engagement, due diligence, processing/ archival/ destruction, security measures, client rights, information governance, sub-contracting, communication with clients.	-	-
		2.3	**2.3** outlines processing activities in scope and covers the lifecycle of the data from collection to destruction. It might make more sense if this came after **2.1** as the processing activities naturally follow on from this.	3. Consider moving **2.3** so processing activities follow **2.1** re. general activities connected with client file.	2.3 moved as suggested COMPLETE Now 2.2
			2.3 refers to 'modification of client data' but it is unclear what exactly this is or how this is addressed in the criteria. Is this related to rectification or something else?	4. Clarify how 'modification of client data' is addressed in the criteria. Add requirements relating to this if necessary.	This is clarified as to where legal service providers update client personal data held in marketing systems due to change of address etc. Rectification text is

					also updated to reflect this with the addition of NB1 COMPLETE (Amendment to N1 at 8.2.4 noted.)
			2.3 – the last bullet ends with a semi-colon but is the last point so should be a full-stop.	5. **2.3** - Replace semi-colon after the last bullet point with a full-stop.	Semi-colon replaced with a full stop. COMPLETE
4. Does the scope set out the UK GDPR responsibilities that are within scope? [Annex 2 ref. 3c.]	Partially	Appendix 1	**<u>Appendix 1 - Controls Table</u>** This lists all the controls, and which is the relevant UK GDPR Article. Some are not mapped to UK GDPR when in fact they relate to accountability, Art 4(2). For example, LOCS:22:C1, LOCS:22:C3, LOCS:22:C5, LOCS:22:C26, LOCS:22:C30, LOCS:22:C33. LOCS:22:C30 is about data sharing between controllers so also relates to Article 26. Article 10 not referenced at all but not listed as out of scope. LOCS:22:C20 for lawful processing only mapped to Articles 6, 7 and 9.	6. Ensure all controls are mapped to all relevant UK GDPR articles in line with comments.	All controls mapped as recommended PARTIALLY Apologies – I incorrectly referenced Article 4 when it should have been Article 5 – Principles. Art 4 is definitions. The references to Art 4 will need to be changed to Art 5.
		Appendix 2	**<u>Appendix 2 – UK GDPR Applicability</u>** This appendix outlines which articles apply to the LOCS standard. Corresponding control references are provided next to each Article, however many of these are not mapped correctly. For example, LOCS:22:C19 is mapped to Art 6 but is about the ROPA, not lawfulness.	7. Review **Appendix 2** to ensure the correct controls are mapped to each UK GDPR Article.	Appendix 2 reviewed and amended PARTIALLY As above Art 4 contains definitions and Article 5 is about the Principles. The references by Art 4 will need to be moved against Art 5.

					Other controls are still listed against the wrong Articles in Appendix 2. For example, LOCS:23:C29 and LOCS:23:30 are listed against Art 44 – 49 which are about International transfers, whereas LOCS:23:C29 and LOCS:23:30 are only about data sharing. As previously mentioned, LOCS:22:C19 is still mapped to Art 6 but is about the ROPA, not lawfulness, as per the 'UK GDPR Reference section of the control table. Also note that the section for each control labelled 'UK GPDR reference' should also be updated to reflect all the UK GDPR articles that apply in line with Appendix 2. For example, 8.4.5 does not cite any articles – see our comment about it relating to Art 26. Ensure all relevant articles are listed in each control section. These should align to Appendix 1 and Appendix 2 and vice versa.
		2.0, intro	In the introductory section ('Processing of Personal Data in the Client File' section) it states, *"The LOCS:22 standard is closely aligned to the UK GDPR requirements for the Processing of Personal Data."*	8. Amend this sentence to say, 'The LOCS standard controls are mapped to the UK GDPR requirements relating to the processing in scope to enable certified organisations to demonstrate compliance with	Sentence amended as recommended. PARTIALLY Sentence amended but reference to relevant Appendix not added.

			As certification against the LOCS standard is intended to verify that the processing in scope complies with UK GDPR, we felt that stronger wording could be used here.	UK data protection law.' or similar. This should then reference the relevant Appendix.	
		2.6	**<u>2.6 UK GDPR areas out of scope</u>** This says Article 8 is out of scope because 'there are no information society services'. This sounds incomplete and it isn't clear whether this means there are no ISS involved in the processing or they are just out of scope.	9. **2.6** - Amend statement in the table to clarify whether Article 8 is out of scope because there are no information societies involved in the processing.	Amended COMPLETE Now 2.5
				10. If information society services are out of scope, they should be included in **2.7** – Processing areas out of scope.	Added COMPLETE Now 2.6
		2.7	As law enforcement processing is not covered by UK GDPR (it is instead covered by Part 3 of the DPA 18) it follows that this processing is not in scope of the scheme. However, given the scheme relates to legal services, and in case providers are caught by Part 3, DPA 18, it is worth explicitly stating that law enforcement processing is out of scope. This will prevent any misunderstandings by people relying on the assurance this scheme provides.	11. Include a statement at **2.7** that law enforcement processing subject to Part 3, DPA 18 is out of scope for this scheme.	Added to 2.7. COMPLETE Now 2.6
			It is not clear what is meant by 'alumni data' in this context, as this generally means graduates or ex-students.	12. Clarify what is meant by 'alumni data'.	Clarified COMPLETE Now 2.6
5. Does the scope allow meaningful data protection certification taking into	Partially	2.0	Some further clarification is needed to ensure this is the case in line with our	*See required actions for this section.*	All recommendations implemented PARTIALLY

account its **nature**, **content**, **risk** and the **scope** of processing? [Annex 2, ref. 2d.]			comments and recommendations above.		Some minor amends required.
6. Does the scope cover personal data processing in the UK, or does it address cross border processing and/or transfers? (**Territorial scope**) [Annex 2 ref. 2e.]	Yes	2.5	Ultimately it is for the scheme owner to decide on the territorial scope. Nevertheless, it is our understanding that the territorial scope of the LOCS scheme is aligned to the territorial scope of the UK GDPR, ie it applies to organisations in the UK and those outside the UK processing personal data relating to data subjects in the UK. However, the wording of the second bullet point at **2.5** does not explicitly say it applies to organisations outside the UK: *"The LOCS:22 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 relate to the offering of legal services (even if free of charge) to Data Subjects situated in the United Kingdom."* Criteria relating to Article 27 are included in the standard for non-UK organisations appointing a representative in the UK, which	13. **2.5** – Clarify whether non-UK organisations subject to the UK GDPR are can also obtain certification under the LOCS scheme. If so, amend the second bullet point of **2.5** to explicitly state that it applies to organisations not established in the UK who are processing personal data relating to the offering of legal services to data subjects who are in the UK in line with Article 3(2). If not, then amend **2.5** and remove criteria relating to non-UK organisations.	Second bullet point in 2.5 amended to clarify for non-UK organisations as recommended. COMPLETE Now 2.4

			further suggests that organisations outside the UK are in scope.		
			The scheme provides for international transfers at **8.4.6**. However, it is not intended to act as a transfer mechanism pursuant to Art 46(2)(f).	-	-
B. Target of Evaluation					
1. Do the scope and/or the criteria **require** a clearly described individual Target of Evaluation (ToE)? [Annex 2 ref. 2f.]	Yes	2.4	Section **2.4** states that the applicant 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…"* It provides a table outlining the information that should be provided.	-	-
i. Where the ToE is not defined by the scope (ie a general scheme), is there a ToE section requiring the controller/processor to define the targeted processing operation (the ToE) in terms of data types, systems and processes used? [Annex 2 ref. 2f.(1)]	Yes	2.4	**2.4** includes requirement to identify data types and high risk data types. Data types provides examples such as contact details and financial details. However our guidance refers to these as *categories* of data.	14. **2.4** - Amend the heading 'data types' to say, 'categories of data.'	Heading amended. COMPLETE Now 2.7
		2.4	Specifically states 'legal technology systems' used. However this doesn't provide for other types of systems; including those used by processors also within scope of the scheme.	15. Widen the heading in the table for systems to allow for all kinds of systems used within the processing operations.	Heading widened COMPLETE Now 2.7

ii. Is the applicant required to define where the processing that is subject to evaluation starts and ends, including all interfaces with other interdependent processing operations? [Annex 2 ref. 2f.(2)]	Yes	2.4	Table in **2.4** requires the applicant to define the 'processing lifecycle'. Although an example is provided, ie *"Client inception to Matter closure"*, it isn't explicit that this is where the processing begins and ends.	16. Amend wording to say, 'Define where the processing begins and ends, eg Client inception to Matter closure.'	Wording amended. COMPLETE Now 2.7.
		2.4	**2.4** doesn't refer to interfaces with other interdependent processing operations, only to "any third party interactions". The ToE should require organisations to identify any interdependent processing operations involved, for example, where there are shared systems.	17. Include a requirement to define any interdependent processing operations and justify them.	Text amended as recommended COMPLETE Now 2.7
iii. Is the applicant required to justify ToE's exclusions and interfaces with interdependent processing? [Annex 2 ref. 2f.(2)]	Yes	2.4	**2.4** says the applicant must justify *"any exceptions (activities to be excluded from the evaluation)."* The table requires information about exclusions although doesn't specifically require justifying it. There is no requirement to justify interfaces with interdependent processing.	18. Include justifying exclusions and interfaces with interdependent processing in the relevant sections of the table. [*Also see **no.15***]	Justification for exclusions and interfaces included COMPLETE Now 2.7
iv. Is the applicant required to identify and reflect special types of processing eg automated decision making, profiling, high risk processing? [Annex 2 ref. 4d.]	Yes	2.4	Table in **2.4** requires the applicant to define 'high risk processing' and provides examples including automated decision making, profiling, and biometric identification.	-	-

v. Is the applicant required to identify the processing of special category/criminal offence data? [Annex 2 ref. 4e.]	Yes	2.4	Neither special category nor criminal offence data are listed here, either under data types or high risk data types. Presumably the intention is that 'high risk data types' is intended to cover special category data as one of the examples is 'medical data'. However the reference to 'high risk data types' may be misleading as this is not something defined in the UK GDPR, neither is it defined in the definitions in section 4. The legislation talks about 'high risk processing' but not high risk data – because it's what you do with it that poses a risk. What UK GDPR does refer to is special category data and criminal offence data which are not mentioned in this section at all. There must be a specific requirement to identify special category and criminal offence data involved in the processing being certified as this determines if and how the certification criteria apply.	19. Reconsider the heading 'high risk data types' to avoid confusion or include a definition of this in **section 4**. If a definition is added then this must include special category data, criminal offence data, and children's data. Alternatively these categories of data could just be included under the heading 'categories of data' as per **no.14**.	Special category and criminal offence now included COMPLETE Now 2.7
				20. Whatever the solution to **no.19** above, include an explicit requirement to identify special category data and criminal offence data.	Included COMPLETE Now 2.7
2. Do the criteria above guarantee that the ToE will be understandable to its audience, including data subjects where relevant? [Annex 2 ref. 2g.]	Yes	2.4	**2.4** - Target of Evaluation section is in between other sections relating to what is in and out of scope. As this is about defining what is to be certified, it might be better to have this at the end of the section so all aspects in and out of scope are dealt with together and come before how the organisation	21. Consider moving Target of Evaluation section to the end of the Scope section **2.0**, for better flow.	TOE section moved as recommended COMPLETE Now 2.7

			must define the processing subject to certification (ToE).		
			Further detail is required in this section to ensure the processing is defined properly for the purpose of certification and so that people ultimately understand what is being certified.	22. Add further detail in line with comments above to ensure the target of evaluation is understandable to the scheme's target audience, including to data subjects.	Comments above implemented COMPLETE
C. General requirements					
1. Are all relevant terms used in the criteria catalogue identified, explained and described? [Annex 2 ref. 3a.]	Partially	4.0	Terms and definitions provided in **section 4.0** are clear and understandable.	-	-
		4.0, 8.3.2, 8.3.3, 8.3.5	'Data Breach' is defined but is more commonly referred to as a 'Personal Data Breach' within the scheme.	23. Ensure terms in **section 4** match those used in the criteria, and vice versa.	All instances of 'Data Breach' now reconciled as 'Personal Data Breach' PARTIALLY Audit reference at 8.3.5 needs updating.
		4.0	'Client' is defined as *"The user of legal services from a Legal Service Provider"* however, this doesn't explicitly say this is an individual rather than an organisation seeking legal services. This impacts the interpretation of the requirements in **section 8.0** which are generally understood as the client being an individual, ie the data subject, as set out in the scope at **section 2.0**, eg *"Processing the Personal Data of the Client."*	24. Amend the definition of 'client' so it is clear this refers to an individual (ie a data subject) rather than an organisation.	Wording amended as requested COMPLETE

		4.0	'Legal Service Provider Supplier' defined but the term is not used within the criteria.	25. Remove definition from **section 4** if term is not used.	Definition removed COMPLETE
		40, 8.1.2	No definition of large scale processing used in DPO section **8.1.2**.	26. Add a definition of large scale processing. This can link to ICO DPO guidance and/or DPIA guidance if necessary, either here or in the relevant section. Also see **no.217**.	Definition added and NB 2 added to **8.1.2** COMPLETE Definition added and note NB3 at 8.1.2.
		4.0, 8.1.3	The term 'Commissioner' is used in the criteria, but this is not defined in **section 4.** Only the ICO is defined. Also see comments re. section **8.1.3**.	27. Consider which terms need to be used in the standard and which ones need to be defined in **section 4**. See actions at **no.154** and **no.155.**	Information Commissioner added to definitions and consolidated in text PARTIALLY Definition added but not sure this accurately defines the role of the Commissioner relating to data protection. It says, *"The Information Commissioner is responsible for providing leadership and strategic direction to the Information Commissioner's Office and acting as Accounting Officer for the Information Commissioner's Office."* Our website says, *"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." which may be better to use.
		4.0	Special category data is defined but not 'criminal offence data'. See other comments about the lack of criteria relating to this category of information	28. Add a definition of criminal offence data. See Criminal offence data | ICO for more information.	Definition added COMPLETE
		4.0, 2.4	'High risk data' is not defined but is used in the ToE section at 2.4. See action **no.19** above.	29. Add definition of 'high risk data' depending on approach taken in response to action at **no.19**.	'high risk' removed from TOE COMPLETE
		4.0, 8.4	Definitions are not always aligned to UK GDPR. For example, 'Joint Controller' is defined as "*Where two or more Data Controllers share obligations and responsibilities for the Processing of Personal Data*". We appreciate that this attempts to simplify/clarify matters, but in doing so risks losing the legal meaning of these words. The key point about joint controllers is that they **jointly determine** the purposes and means of processing of personal data. Our guidance says, *"If two or more controllers jointly determine the purposes and means of processing the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes."* Also see, What are 'controllers' and 'processors'?	30. Ensure the definition of 'joint controller' is aligned to UK GDPR and ICO guidance and that this is accurately reflected in the joint controller obligations in **section 8.4**.	Joint Controller definition amended. 8.4 updated COMPLETE Definition and 8.4.2, NB3 amended

		4.0	Definition for 'Personal data' has an unnecessary apostrophe at the beginning before 'means'.	31. Delete apostrophe before the word 'means'.	Apostrophe deleted COMPLETE
2. Are all normative references identified? [Annex 2 ref. 3b.]	Yes	3.0	Section 3.0 – Normative References. 3.1 Legal Services Operational Privacy Certification Scheme (LOCS) – LOCS standard 3.2 Legal Provisions – GDPR/DPA 18 3.3 Related National Standards 3.4 ICO Guidance – provides links to relevant guidance. 3.5 Other documents – various EDPB, WP 29 docs, and ICO docs/guidance.	-	-
			8.3.8.3 refers to the 'Department of Defence standard' but doesn't explain what this is, and it isn't included in the normative references or definitions.	32. Include details of the 'Department of Defence standard' in the normative references.	Now replaced by NIST 800-88 standard included in normative references COMPLETE
		3.1	**3.1** - It doesn't seem necessary to list the LOCS:22 Standard as a normative reference as the intention of these references is to list *other* documents that are necessary to understand the criteria document. It may be necessary to list any other scheme documents that are not involved in the review – perhaps scheme rules or auditor notes.	33. Delete **3.1** unless there are other scheme documents it is appropriate to include here.	Removed COMPLETE
		3.4	**3.4 - ICO guidance** – It is fine to use ICO material published on our website but the use of these links here and wording within the document might be subject to the Open Government Licence. Our webpage on Copyright and re-use of materials | ICO says:	34. Include the attribution the ICO in line with our comment here. This could be included as a statement preceding or following the list of ICO guidance. For example, 'The ICO guidance and materials cited	Statement added after the guidance. COMPLETE

			'All text content on this website is available under the Open Government Licence (OGL) v3.0, except where otherwise stated. If you re-use text content under the OGL, you must include the following attribution: Information Commissioner's Office, [name and date of publication], licensed under the Open Government Licence.'	here or referred to within the standard are licensed under the Open Government Licence', or similar.	
		3.5	**3.5 - Other documents** - There is a designated list for ICO Guidance so it's not necessary to include reference to ICO guidance and checklists in this list. If it is necessary to refer to ICO guidance more generally then it should rather be included in **3.4**.	35. **3.5** - Either delete references to ICO guidance or move to **3.4** as appropriate.	Reference deleted from 3.5 COMPLETE
			It seems unlikely that all 'other documents' referenced in **3.5** are relevant to the scheme. For example, opinion on facial recognition and guidelines on the application and setting of administrative fines. We are not familiar with the Data Ethics Framework, but it appears to have been updated in 2020 (not 2018) and is targeted at government and public sector which would not likely be in scope for the LOCS scheme.	36. **3.5** - Check all the references listed and only include those that are relevant for the scope of the LOCS standard. Ensure all references cite the latest version of the document.	References updated COMPLETE
3. Where other standards are cited – do criteria allow for interaction with those standards?	Partially	3.3	Standards in **3.3** appear to be referenced for information and are not cited in the standard as being a way of fulfilling any of the criteria. For	37. If the Department of Defence Standard is included in requirements at **8.3.8.3**, ensure the relevant criteria are	DOD is replaced by NIST standard – all other 8.3.8 controls are cross referenced to ISO 27001 and/or Cyber Essentials where appropriate

[Annex 2 ref. – N/A]			example, certification under ISO 27001. See earlier comment and action at **no.32** about the Department of Defence Standard. If this is a requirement, then it will be necessary to ensure they are compatible and certification body's audit requirements reflect that.	compatible with that standard and vice versa.	PARTIALLY Notes for **8.3.8.1, 8.3.8.2** and **8.3.8.6/7** include notes that says the criteria are met if ISO27001/cyber Essentials are 'in place'. It's not clear what is meant by that. Would an organisation be required to be certified under these standards or merely follow the standard? Section 7.4 of the UK additional accreditation requirements says *"In addition to item 7.4.5 of ISO 17065, it shall be provided that existing certification, which relates to the same object of certification, may be taken into account as part of a new evaluation. However, the certificate alone will not be sufficient evidence and the certification body shall be obliged to check the compliance with the criteria in respect of the object of certification. The complete evaluation report and other relevant information enabling an evaluation of the existing certification and its results shall be considered in order to make an informed decision. In cases where existing certification is taken into account as part of a new evaluation, the scope of said certification should also be assessed in detail in respect of*

					its compliance with the relevant certification criteria." ISO 17065, s.7.4.5 says, *"The certification body shall only rely on evaluation results related to certification completed prior to the application for certification, where it takes responsibility for the results and satisfies itself that the body that performed the evaluation fulfils the requirements contained in 6.2.2 and those specified by the certification scheme."* What this means in practice is that it's not possible to rely on the certification as evidence without the CB checking that it has been assessed as being implemented and it relates to the same processing (target of evaluation). Until the audit rules for this are set it may be better to keep this more open, eg certification to ISO 27001/Cyber Essentials for the processing within scope may 'be accepted as evidence of compliance in certain circumstances'/ 'be a way of evidencing compliance with this requirement/ 'contribute towards…', or something to that effect.
Specific topics to be considered					

Comments should include reference to how effectively the criteria contribute to the objectives of the certification scheme. If topics are not covered or not applicable (partially or wholly) by the criteria, please provide reasons. These are not exhaustive – extend topic where appropriate or create new topic at the end.					
D. Principles, Article 5					
Do the criteria adequately address all data protection principles outlined in Article 5? *(NB. Some of these are covered in more detail in other sections)* [Annex 2 ref. 6a.]	Partially	8.1.4	Principles are covered in **8.1.4**. Each one is dealt with in turn. However, whereas some of the principles are covered in more detail elsewhere in the document, some are only covered here, and the controls do not always set adequate requirements where that is the case. For example: • purpose limitation (see comment below) doesn't include considerations from Article 6(4) about what constitutes compatible purposes. • storage limitation - there is no requirement for data to be regularly weeded in line with this policy.	38. Some of the criteria need expanding to ensure they set robust requirements relating to the principles, or additional sections adding to the criteria ensuring specific requirements are set for all the principles. See our guidance on The principles *Also see comments and actions below for each of the principles.*	All principles cross related to relevant controls COMPLETE Certain principles expanded PARTIALLY – some need tweaking – see comments below. Storge limitation linked to 8.1.7.7 for 'weeding' COMPLETE Links to ICO guidance added to all principles COMPLETE
			Each of the principles has specific controls: **8.1.4.1** – lawfulness, fairness and transparency **8.4.1.2** - purpose limitation **8.4.1.3** – data minimisation **8.4.1.4** – accuracy **8.4.1.5** – storage limitation **8.4.1.6** – integrity and confidentiality/security **8.4.1.7** – accountability Some of these are only covered in this section whilst some are covered in more detail elsewhere. However, that	39. Where there are requirements elsewhere in the document that relate to the principles, eg lawfulness and transparency (**8.3.4** and **8.2.2**), data minimisation (**8.3.1**), storage limitation (policy at **8.1.7**), security (**8.3.7** and **8.3.8**), cross-reference the relevant sections. For example at **8.1.4.1** could be reworded to say, 'Client file data shall be processed...in line with sections **8.3.4** and **8.2.2**.'	Section **8.1.4** has been amended in line with recommendations. PARTIALLY All principles cross referenced to relevant controls. Additional criteria added. A few minor amends necessary in line with comments below.

			isn't made clear as the other relevant sections are not cross-referenced in **8.1.4**. **Lawfulness and transparency** are covered in **8.3.4** and **8.2.2**; **Purpose limitation** and **data minimisation** are also covered in data protection by design & default section at **8.3.1**; **Accuracy** isn't covered anywhere else (other than if a DS exercises their rights and disputes the accuracy); **Storage limitation** is covered in relation to the retention and destruction policy at **8.1.7**, but nothing else (other than secure disposal in security section) – see comment below; **Security** is also covered extensively in **8.3.7** and **8.3.8**.		
			The **2nd introductory sentence** says, 'Organisations that apply these core principles to their Processing activities will be going a long way towards meeting UK GDPR requirements.' However, as complying with the principles is a legal obligation it seems unnecessary to say that.	40. Either amend this sentence to reflect that organisations must process personal data in line with the data protection principles or delete.	Amended sentence to reflect recommendation. COMPLETE
		8.1.4, data processor alternative control	The data processor alternative control says **8.1.4** applies equally to processors, however, that is not necessarily the case. For example, Art 5(2) says "the controller shall be responsible for…", and for the first principle the controller establishes the	41. Consider whether principles apply to processors and if so how. Amend the alternative control accordingly. It may be helpful to look at our detailed guidance on <u>What does it mean if you are a processor?</u>	Processors section updated PARTIALLY Updated in line with recommendation but the requirement isn't numbered.

			lawful basis and provide privacy information – the processor can only process on instructions from the controller. For storage limitation they will return or delete data at the end of the processing period as determined by their contract. Because processors can only process data in line with instructions from the controller – everything relating to their processing is determined by the contract rather than the principles. The data processor alternative control explains to processors, "If you act outside your instructions or process for your own purposes, you will step outside your role as a processor and become a controller". This note isn't particularly helpful and misses the important point that if they are a processor and act outside the instructions of the controller they would be in breach of contract and the processing may not be lawful. They also risk regulatory action by the ICO.	If all the processor obligations outlined in this guidance are covered elsewhere in the criteria, it may be better to just disapply this section. Another option could be to include alternative requirements that they: • act on the instructions of the controller, • notify the controller if any of their instructions would lead to a breach of UK data protection laws, and • assist the controller in meeting their data protection obligations.	This section also includes what appears to be an explanatory note but is not annotated as such, eg NB 20. **NB** – This applies elsewhere. There are also notes in some processor alternative control sections, eg here and **8.2.1**, but these also don't have reference numbers. Ensure a consistent approach throughout. All requirements must have a reference number, including those for processors. *Check all and amend accordingly.
5.1(a) Lawfulness, fairness and transparency	Partially	8.1.4.1	This is the first time lawful is mentioned and the need for additional lawful basis for special category data or criminal offence data is not included. This may be because lawfulness is covered in more detail at **8.3.4** but this isn't clear as that section is not referenced. See comments above about this.	42. Determine if **8.1.4.1** should include the need to identify an additional condition for processing for processing special category and criminal offence data, or if this can be resolved by cross-referencing **8.3.4**.	**8.3.4** cross-referenced. COMPLETE

			Lawfulness is not only about having a lawful basis, but whether the processing is generally lawful. For example, our guidance says, "*Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense…*"	43. Ensure **8.1.4.1** and the corresponding guidance notes reflect ICO guidance on the lawfulness, fairness and transparency principle.	Section updated and cross referenced COMPLETE Additional note added at NB 1 and ICO guidance linked at NB 4.
		8.1.4.1, NB 1	The guidance note at **NB 1** refers to 'for the purposes of a contract', however this doesn't reflect that the processing must be **necessary** for the fulfilment of the contract. See our comments later about necessity in our comments for **8.3.4**.	44. Ensure **NB 1** reflects necessity of processing for it to be lawful (apart from consent). See also comments and actions re. **8.3.4**.	Amended NB 1 to reflect necessity of processing. PARTIALLY Amended but not sure about wording: *"…there must be a lawful basis for Processing Client Personal Data, and a necessity of processing for it to be lawful (apart from 'consent')..."* Suggestion: '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…'

5.1(b) Purpose limitation	Yes	8.1.4.2	This only has one requirement for purpose limitation which does not seem proportionate given that function creep is a real data protection concern. Although purpose limitation is referred to in **8.3.1**, there is no consideration of what constitutes compatible purposes pursuant to Art 6(4).	45. Include considerations from Art 6(4) regarding compatible purposes. This could be included as a requirement, or a note, or in the lawful processing section at **8.3.4**. Also see our guidance on Principle (b): Purpose limitation	Compatibility requirements added COMPLETE
5.1(c) Data minimisation *[Do the criteria specifically require demonstration of data minimisation for the individual ToE (processing activity)?]* [Annex 2 ref. 6b.]	Yes	8.1.4.3	Data minimisation is covered briefly here but is also covered in **8.3.1**. about data protection by design and default.	46. See comments re. **8.3.1** and also **no.38** about cross-referencing other relevant sections.	Cross-referenced as recommended. COMPLETE
		8.1.4.3, NB 5	**NB 5** says that any surplus data provided by the Client should be deleted but no further guidance given. As information should be deleted in line with the Retention and Destruction policy it would be helpful to cross-reference that policy here.	47. Cross reference the Retention and Destruction policy here.	Cross-referenced as recommended. COMPLETE
			NB 5 uses 'shall' and is therefore a requirement. To be compatible with ISO 17065 guidance notes must not contain requirements. In this case we think that it would be more appropriate to include the note as a requirement.	48. Include the note from **NB 5** as a requirement in the control section.	Moved first line of **NB 5** to the control section. COMPLETE
5.1(d) Accuracy	Partially	8.1.4.4	Covered at **8.1.4.4** and **NB 6**, however this section could go further to reflect our guidance on Principle (d): Accuracy, for example clearly identifying opinions.	49. As this is only place setting requirements for accuracy, ensure it reflects the ICO's expectations set out in our guidance on Principle (d): Accuracy.	Opinions added cross reference to right to rectification added PARTIALLY

			Recommendations are made to periodically confirm with the Client that all Personal Data held on file is up to date and accurate and provide a self service portal. Whilst we would certainly expect that organisations periodically review accuracy of the data, checking with the client that all information held is accurate may not be feasible as presumably there will be a lot of information in the file, and potentially not all of it provided by the client? An organisation may rather check specific information or a sampled selection.		**8.1.4.9** says 'take reasonable steps'. This could be reworded to remove subjective term, eg 'Take steps to ensure…' **8.1.4.9(d)** should cross-reference **8.2.4** for completeness. **8.1.4, NB12** says that "Data subjects have the absolute right to have incorrect personal data rectified". This is not strictly true – the only absolute right is to object to direct marketing. Requests can be refused by the controller in certain circumstances, for example where an exemption applies. They may also choose to add a statement that the data is inaccurate rather than correct it as there may have been a course of action that took place on the basis of the original data and there needs to be a record of that. Suggest including reference to **8.2.4** at **8.1.4.9(d)** and deleting **NB 12**.
5.1(e) Storage limitation (retention)	Partially	8.1.4.5	This does not go beyond the stipulation at Article 5.1(d). The Retention & Destruction policy at **8.1.7** is not referenced and there is no requirement for data to be regularly 'weeded' in line with this policy.	50. In addition to **8.1.4.5**, include a separate requirement to regularly review and delete data in line with this policy. For example, 'Retention of Client file data shall be managed in line with the Retention &	Control added after **8.1.4.5** as recommended PARTIALLY Now **8.1.4.10** with new requirement added at **8.1.4.11** as requested. Reference to **8.1.7** added.

				Destruction Policy outlined at **8.1.7**.' See also our guidance on Principle (e): Storage limitation and the Records management and security section of our accountability framework.	Are there any circumstances where any personal data would need to be kept for public interest archiving, scientific or historical research, or statistical purposes? If so, this should be clearly identified. If not, this should be clearly stated. For example, you have mentioned 'alumni data'. Is this in the individual's expectations? Personal data should only be kept for as long as it is necessary for the stated purpose, eg to provide legal advice. It should not be kept just in case it might be useful in the future. NB. this could be addressed here or in **8.1.7**.
5.1(f) Integrity and confidentiality (security)	Yes	8.1.4.6	This subject is dealt with in significantly more detail in the security sections at **8.3.7** and **8.3.8** but this is not clear as they aren't referenced.	51. **8.1.4.6** - Cross-reference the security section at **8.3.7** and **8.3.8**.	(Now **8.1.4.7**) Cross-referenced as recommended. COMPLETE Now 8.1.4.12. sections cross-referenced.
5.2 Accountability	Partially	8.1.4.7, NB 9	**NB 9** explains what records can be used to demonstrate accountability. These are items required elsewhere in the document, but relevant sections are not referenced.	52. **8.1.4.7, NB 9** – cross reference the relevant section for each of the items listed.	All relevant sections now cross-referenced. COMPLETE
		8.1.1, 8.1.3, 8.1.5, 8.3.9,	Accountability also covered in other requirements relating to information governance, for example **8.5** but Article 5(2) is not referenced. For	53. Ensure accountability principle [Art 5(2)] is referenced in all sections that are intended to assist organisations in demonstrating accountability.	All sections that form part of accountability cross referenced as recommended NOT COMPLETE

		8.4.1. 8.4.5, 8.5.	example, **8.1.1, 8.1.3, 8.1.5, 8.3.9, 8.4.1. 8.4.5, 8.5**.		This was about referencing Art 5(2) in the 'UK GDPR REFERENCE' section of **8.1.1, 8.1.3, 8.1.5, 8.3.9, 8.4.1** or **8.5** which does not appear to have been addressed.
E. Lawfulness of processing (Art 6 – 10)					
1. Do the criteria require checking the lawfulness of processing for individual processing operations with respect to purpose and necessity of processing? (Including Art 6(4) re. compatible purposes) [Annex 2 ref. 5a.]	Yes	8.3.4, intro	**8.3.4 Lawful Processing** Each lawful basis is covered in its own subsection within 8.3.4. The section introduction states that "*Where Client Personal Data is Special Category the default position for an Organisation is that they do NOT process this data unless a UK GDPR Article 9 condition for Processing is met and documented*." The wording should be stronger than 'default position' as the processing will not be compliant with DP legislation if an Article 9 condition is not in place. In addition there is no reference in the introduction to criminal offence data and the conditions for processing that information.	54. a) Amend wording to make it clear that an Article 9 condition for processing must be in place if processing special category data. b) Include expectations for criminal offence data in the introduction.	Wording amended NB 3 reference and link to Schedule 1 DPA 2018 added COMPLETE
		8.3.4	**8.3.4** starts with a requirement for not processing special category data unless an Article 9 condition is met. However, the first thing an organisation must determine is whether they can identify a valid lawful basis from Article 6. Whilst this is covered in the introduction and to an extent for each individual lawful	55. **8.3.4** – Before the requirement for special category data, include an overarching requirement here to establish and document a lawful basis from Art 6 prior to processing commencing. The corresponding requirement for each lawful	Requirement added as new **8.3.4.1** as recommended. COMPLETE

			basis, it would make more sense to begin this section with an overarching requirement for complying with Art 6 before the requirement for special category data.	basis could then refer back to this.	
			Other than consent, all the lawful bases require the processing to be *necessary* for that particular purpose, eg 'processing is *necessary* for the performance of a contract…'. However, the necessity of the processing is not fully addressed in this section. For example, **8.3.4.7** just requires the organisation to identify and document why contract is relevant lawful basis. Necessity is mentioned in the notes at **NB 5, 6, and 7** but not in the controls section and not in the notes for all the bases where necessity should be a consideration.	56. **8.3.4.7, 8.3.4.9, 8.3.4.10, 8.3.4.12, 8.3.4.14** - To ensure necessity of the processing is considered, the first requirement for each lawful basis could be amended to say, 'The organisation shall document why XXX is the most appropriate lawful basis and how the processing is necessary for that basis.' Or similar. Alternatively another requirement could be added into each sub-section of **8.3.4** re. Article 6(1)(b)-(f) to assess and document how the processing is necessary.	Relevant controls have been amended to emphasise establishing necessity of lawful basis as recommended. COMPLETE Added to the first requirement in each section using first suggestion.
			It seems unlikely that all lawful bases or conditions for processing will be relevant for the processing in scope, for example public task). Therefore, it would be helpful to provide more specific guidance, relevant to the processing, in the guidance notes.	57. Tailor the guidance notes to the processing in scope, for example indicating where a lawful basis or condition for processing won't/may be unlikely to apply. If public task is out of scope this should be included at **2.6**.	Where lawful basis is unlikely this has been indicated Public task may not be out of scope if the certifying organisation is the legal department of a public authority COMPLETE
		8.3.4, NB 1	As the shortened forms of the lawful bases are used in the subsequent	58. Consider introducing the commonly used shortened	**NB 1** amended as recommended.

			requirements pertaining to each lawful basis, eg 'public task', it might be useful to introduce those terms in brackets in this list.	terms for each lawful basis, ie 'consent', 'contract', 'legal obligation', 'vital interests', 'public task', 'legitimate interests' in brackets after each explanation in this list.	COMPLETE
2. Do the criteria require checking all the conditions of a legal basis for individual processing operations are met, including conditions for special category data? [Annex 2 ref. 5b., 4a.]	Partially	8.3.4	**8.3.4** - Each lawful basis is dealt with separately – setting requirements for meeting the conditions of each. See comments below.	-	-
		8.3.4.1	**8.3.4.1** says the "organisation shall not process Special Category Data unless one of the UK GDPR Art 9 conditions for Processing is met and documented." **NB 2** lists the conditions for processing special category data, but there is no mention of the additional conditions and safeguards set out in Schedule 1 of the DPA 2018 . As this is the only requirement relating to establishing lawfulness of processing for special category data this is not sufficient.	59. Include specific requirements for special category, as far it is relevant to the processing in scope; including the further conditions set out in Schedule 1 of the DPA 18 relating to some of the Art 9 conditions. See our guidance on special category data for more information.	Reference to Schedule 1 DPA conditions and 'appropriate policy document' added PARTIALLY **8.3.4.2** refers to **NB 1** for Art 9 conditions but these are in NB 2. *Amend reference. **8.3.4.4** refers to Art 9 (b), (h), (I), and (j) but not Art 9(g) which is the substantial public interest condition. This appears to be an oversight. If not, this should be included. In that case the requirement for an Appropriate Policy Document at **8.3.4.5** which is needed for all Sch.1, Part 2 (substantial public interest) conditions should also be updated. If this has been omitted for a reason, then this should be explained and excluded from scope.

					NB. **8.3.4.2** and **8.3.4.3** say *"SHALL not"*. It would be better if the 'not' as also in red capitals to ensure the requirement not to do something is as obvious as when to do something. This also applies to 8.2.1.3, 8.2.3.5, 8.2.5 - NB 4, 8.2.6.5, and 8.2.9.3.
		8.3.4	There are no requirements for processing criminal offence data in **8.3.4**. As this is not documented as out of scope, and seems relevant to legal client services, this appears to be an omission. There should be requirements for ensuring processing of criminal offence data is lawful in line with Article 10 and DPA 18, schedule 1.	60. Include requirements for criminal offence data, as far as it is relevant to the processing in scope; including the further conditions set out in Schedule 1 of the DPA 18 relating to the processing of such data. See our guidance on Criminal offence data.	Criminal offence Data requirements added COMPLETE
		8.3.4	The DPA 2018 outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category and criminal offence data under certain specified conditions. Almost all the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require organisations to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).	61. The requirements for special category and criminal offence data must reflect the need for an Appropriate Policy Document in some circumstances.	Appropriate policy document referenced Schedule 1 Part 4 retention requirements added PARTIALLY Requirement for APD added, however, see comment above re. action **no. 59** about public interest conditions.

			This document should demonstrate that the processing of special category and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it should outline the retention policies with respect to this data. (See Schedule 1 Part 4).		
		8.3.4.2 – 8.3.4.6	**8.3.4.2 – 8.3.4.6** relate to '**consent'**. See specific comments below.	-	-
			It seems unnecessary to refer to 'Art 6(a) consent' for each requirement. This also applies to the other lawful bases.	62. Options: **a)** If consent is defined in **NB 1** then reference to Art 6(a) could be removed. **b)** As each requirement in this section begins with 'Where Art 6 (a) 'consent' is used…', this could be pulled out and follow with a bulleted list of requirements, eg: 'Where Art 6 (a) 'consent' is used: i) The organisation shall… ii) The organisation shall… iii) Etc **c)** Include reference to Art 6(a) after the word 'Consent' in bold at the beginning of the requirements, eg 'Consent [Art 6(a)]' **NB. This also applies to the subsequent sections for other lawful bases.**	Requirements amended using option A as recommended. COMPLETE
		8.3.4.3	**8.3.4.3** says 'present the request' but doesn't explicitly say for what.	63. For the avoidance of doubt, amend to say, 'present the request for consent'.	Amended as recommended. COMPLETE

			Presumably this is the request for consent.		*Now 8.3.4.8*
		8.3.4.6(b)	**8.3.4.6(b)** says 'An affirmative action' but this doesn't quite fit with the opening statement for the list, ie it would read 'Any consent given SHALL be an affirmative action'.	64. **8.3.4.6(b)** - Amend to say 'Indicated by an affirmative action…' so it fits with the opening sentence.	Amended as recommended. COMPLETE *Now 8.3.4.11(b)*
		8.3.4.7 – 8.3.4.8	**8.3.4.7 – 8.3.4.8** relate to '**contract**'. See specific comments below.	-	-
		8.3.4.7	As per comments above, it seems unnecessary to refer to the legislation.	65. See **no.62**	Amended as per no.62 COMPLETE
		8.3.4.7	As per comment above - doesn't deal with necessity of processing, or which contract it is necessary for.	66. **8.3.4.7/8.3.4.8** - Include the requirement to document which contract the processing is necessary for, regardless of the number of contracts in existence. See also **no.56**.	Amended **8.3.4.7** (now **8.3.4.8**) to add 'what contract is being used' in line with recommendations. COMPLETE
		8.3.4.8	How this is written it only applies where more than one contract exists, but as mentioned above it in important to document which contract the processing is necessary for, thereby justifying the lawful basis regardless of whether there is one or more that one.		See above. COMPLETE
		8.3.4.9	**8.3.4.9** relates to '**Legal obligation'.**	-	-
			As per comments above, it seems unnecessary to refer to the legislation.	67. See **no.62**	Amended as per no.62. COMPLETE
			8.3.4.9 says, '…by specifying which law is applicable and why the Processing is	68. Replace the word 'relevant' with 'necessary'. This should address the point above at **no.56**.	Amended as recommended. COMPLETE

			relevant.' This should be about necessity of processing not relevance.		
		8.3.4.10 – 8.3.4.11	**8.3.4.10 – 8.3.4.11** relate to '**vital interests'**.	-	-
			As per comments above, it seems unnecessary to refer to the legislation.	69. See **no.62**	Amended as per no.62. COMPLETE
		8.3.4.12 – 8.3.4.13	**8.3.4.12 – 8.3.4.13** relate to **'public task'**.	-	-
			As per comments above, it seems unnecessary to refer to the legislation each time.	70. See **no.62**	Amended as per no.62. COMPLETE
		8.3.4.14 – 8.3.4.19	**8.3.4.14 – 8.3.4.19** relate to **'legitimate interests'**.	-	-
			As per comments above, it seems unnecessary to refer to the legislation each time.	71. See **no.62**	Amended as per no.62. COMPLETE
			Our guidance for legitimate interests and recital 50 says, if an organisation's purposes change over time or they have a new purpose which they didn't originally anticipate, they 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. As it seems possible that legitimate interest will be used by organisations in scope for activities such as sharing information or marketing (referred to at **8.1.4.1**), the requirements and	72. Include additional requirements and/or guidance on the use of legitimate interests where there is a change in purpose.	Guidance added as to potential for use of LI for compatible processing COMPLETE

			guidance notes in this section should reflect this.		
		8.3.4.15	**8.3.4.15** does not deal with necessity. Also see other comments above.	73. **8.3.4.15** – reword to say, 'Where Art 6 (f) '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.' Also see **no.56**.	Amended as recommended. COMPLETE
		8.3.4.16	**8.3.4.16** covers clients being 'fully informed' as to how their data will be processed but doesn't set a requirement to specify the legitimate interests being pursued. This is a legal requirement.	74. **8.3.4.16** - Expand this requirement to include documenting the specific legitimate interests in the privacy notice and cross-reference the requirement relating to that re. Art 13/14.	Requirement expanded as recommended by adding line 'An Organisation SHALL document the specific Legitimate Interests in the privacy notice as laid out in **8.2.2**.'. COMPLETE
		8.3.4.18	**8.3.4.18** sets a requirement to conduct a legitimate interest assessment but makes no reference to this being a three part test in line with ICO guidance Legitimate interests | ICO	75. **8.3.4.18** – expand to say this is a three part test where they need to: 1. identify a legitimate interest (purpose test); 2. show that the processing is necessary to achieve it (necessity test); and 3. balance it against the individual's interests, rights and freedoms (balancing test).	Expanded as recommended. COMPLETE *Now 8.3.4.23*
		8.3.4, NB 8	**NB 8** provides a link to ICO guidance (which incidentally is broken). However, to help organisations understand more about the balancing test, it might be worth some extra notes here about LI more generally.	76. Update the link to Records of processing and lawful basis and consider adding more guidance notes in line with comments here and linking to other relevant guidance such as the more general guidance on	Link fixed, other recommendations implemented COMPLETE

			For example, regarding the balancing test - "If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests." Also that "the legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits."	legitimate interests which also provides guidance on the LIAs. We also have detailed guidance on conducting an LIA, including a template.	
		8.3.4, NB 9	The guidance as to when lawful bases are likely to be used is helpful. However, consider if updating the client on work progress would fall under legitimate interest. It seems it would be more likely to fall under contract – as often (for solicitors) letters of engagement specify when/how often their clients will be updated on work progress.	77. Consider whether updating the client on work progress would fall under legitimate interest, or contract.	Changed to informing clients of related seminars/publications COMPLETE
F. Data subject rights (Art 12-23)					
1. Do the criteria cover transparent information, communication and modalities for exercising rights? (Article 12)	Partially	8.2, intro	**8.2** contains requirements relating to data subject rights. The intro to this section says that "Demonstrating the ability to provide and honour these rights promotes trust and enhances the Client experience." However, observing the privacy rights of individuals is more than a question of enhancing the client experience - it's a legal obligation.	78. Amend the intro to **8.2** to reflect the fact that the organisation is legally obliged to uphold individual's data protection rights, and by complying with these requirements they can demonstrate they have fulfilled those obligations.	Amended as recommended. COMPLETE

		8.2	Throughout **8.2** the term 'Client' and 'Data Subject' are used inconsistently which is confusing as it's not clear if a distinction is being drawn between the exercise of rights by one or the other. It is important to note that all data subjects can exercise their rights against a controller and in some cases, this may not be the client. For example, the organisation may be processing personal data in the client file relating to third parties who are also within their rights to request their information.	79. Ensure the requirements throughout **8.2** reflect the fact that it may not always be the client exercising their rights. For example, this could be addressed by replacing all instances of 'client' in this section with 'data subject'. This should also be clear in the intro. NB. this will also affect section **8.3.6** re. 'Client Rights management' – see **no.80**.	All instances of client replaced with data subject as recommended for **8.2** and **8.3.6**, including title changes for the relevant sections and appendices. PARTIALLY Now refers to 'data subject' rather than 'client' re. rights in both **8.2** and **8.3.6**. However, **Appendix 1** still refers to Client rights rather than DS rights. Check if this also needs amending. We mentioned making it clear in the intro about the fact individuals other than the client may exercise their rights where their information is being processed. While it now refers to clients *and* data subjects, it doesn't explicitly state this. Instead, it may be helpful to add a note in the 'control application guidance' section explaining this for the avoidance of doubt.
		8.3.6	**8.3.6** covers 'Client Rights management'. As for the above comment – any data subject can exercise their rights, and this may not always be the client. Unless it is intended that there will be a separate process for other data subjects then	80. Ensure **8.3.6** reflects the fact that all data subjects can exercise their rights, including the client and other third parties whose data is contained within the client file. Also see **no.79**.	See above. COMPLETE

			this section should be updated to reflect that.		
		8.2.1	**Article 12** is covered in **8.2.1** – 'Transparency & Communication'.	-	-
		8.2.1.6	**8.2.1.6** says, '…the request by electronic form means' which doesn't really make sense.	81. Reword **8.2.1.6** to say 'the request by electronic means'.	Amended as recommended. COMPLETE
			8.2.1.6 goes on to say, 'in commonly used electronic form', but we think this should say 'format'.	82. Replace 'form' with 'format'.	Amended as recommended. COMPLETE
		8.2.1.7	**8.2.1.7** - This is a very long sentence covering multiple points but has very little punctuation to break it up.	83. **8.2.1.7** - Include some punctuation to break up the sentence a bit more and make it easier to understand and audit against.	Sentence edited COMPLETE
			Says '…inform the data subject…on the possibility of lodging a complaint with the commissioner…' which should be reworded.	84. Replace 'on' with 'about'.	Amended as recommended. COMPLETE
		8.2.1.11, NB 4 and throughout	Refers to DPA 2018 Part 8, Schedule 2. Part 8 is not listed in the updated version of the DPA 18, and this should be amended. Exemptions are covered in Schedules 2-4 of the DPA 18 NB – this also applies to other sections of the certification standard e.g. **8.2.2** and **8.2.3**.	85. Remove all references to 'part 8' of the DPA 18. This particular reference re. exemptions should refer to schedules 2-4 of the DPA 18.	All references to Part 8 removed. COMPLETE
		8.2.1, NB 2	**NB 2** says, '…has a right to request responses audibly.' Should this rather be 'verbally'?	86. **NB 2** - Replace 'audibly' with 'verbally'.	Amended as recommended. COMPLETE

		8.2.1, NB 3	**NB 3** Says, '…documents be passworded' instead of password protected.	87. **NB 3** – change 'passworded' to 'password protected'.	Amended as recommended. COMPLETE Amended but moved to requirements section at **8.2.1.14**.
2. Do the criteria adequately address data subject's **right to be informed** and require respective measures to be implemented? (Art 12-14) [Annex 2 ref. 8a., 10h.]	Partially	8.2.2.2	**8.2.2.2** contains requirements relating to Article 13.	-	-
		8.2.2.2(d)	This doesn't stipulate that the controller should explain what the legitimate interests are in the privacy notice.	88. Amend to say, 'where the Processing is based on legitimate interests, details of the legitimate interests pursued by the Organisation or by a third party' to ensure Article 13 is accurately reflected. See also comment re. Art 14 at **no.93.**	Amended as recommended. COMPLETE
		8.2.2.2(f)	We acknowledge that the wording used in **8.2.2.2(f)** about providing information about international transfers is largely taken from the legislation, but it isn't very easy to understand.	89. Rather than trying to cover all the information to be provided about transfers at **8.2.2.2(f)**, it might be better to use the simplified wording from our guidance, ie: 'The details of transfers of the personal data to any third countries or international organisations' Then a guidance note could be added to explain that organisations should say whether the transfer is covered by adequacy regulations. And if the transfer is not made on the basis of an adequacy decision, they should give people brief information on the safeguards	8.2.2.2(f) simplified and guidance note added PARTIALLY Wording amended but not quite as suggested. This says, *"where applicable, that the Organisation intends to transfer Personal Data to a recipient in a third country or international Organisation and the means to obtain a copy of any safeguards where they have been made available."* If this is still to be included, rather than covered in the new note at **NB 5** as suggested, then it needs to say, '…the means to obtain a copy of any safeguards

				put in place in accordance with Article 46, 47 or 49 of the UK GDPR. Including how to get a copy of the safeguards.	**or** where they have been made available.' Either reword **8.2.2.2(f)** and **NB 5** in line with original recommendation (highlighted) or amend in line with comment above.
		8.2.2.2(h)	This is similar to point **8.2.2.3(i)** re. Article 14, but the wording in **8.2.2.3(i)** is clearer.	90. **8.2.2.2(h)** - Replace with the wording from **8.2.2.3(i)**	Amended as recommended. COMPLETE
		8.2.2.2(i)	This says processing based on consent but then quotes the relevant UK GDPR Articles. This approach is not used for legitimate interests at **8.2.2.2(d)** - or below re. Art 14. It isn't really necessary to quote the articles and the same approach should be used for all.	91. Consider whether it's necessary to quote the articles when referring to the lawful basis. Use the same approach for all similar requirements.	Reference to articles removed. COMPLETE
		8.2.2.3	**8.2.2.3** contains requirements relating to Article 14.	-	-
		8.2.2.3(f)	Same as Art 13 requirements at **8.2.2.2(f)** re. international transfers.	92. Amend in line with recommendation for **8.2.2.2(f)**. Also see **no.89**.	Amended in line with 8.2.2.2 (f) PARTIALLY See comment at **no.89** above.
		8.2.2.3(h)	Same as for **8.2.2.2(d)** re. specifying legitimate interests being pursued.	93. Amend in line with recommendation for **8.2.2.2(d)**. See **no.88**.	Amended as recommended. COMPLETE
		8.2.2.3(j)	The word 'consent' isn't capitalised as for the corresponding requirement at **8.2.2.2(i)**. We noted inconsistencies in capitalisation of 'consent' throughout the document. In the document	94. Ensure consistent use of capitalisation of specific terms throughout the document.	Capitalisation of consent now consistent throughout document. COMPLETE

			generally, the capitalised terms appear to be those that are defined in section 4.		
		8.2.2.6	**8.2.2.6** says the organisation shall **process** all requests in line with **8.2.1** whereas the equivalent requirements for the other rights say **respond** to all requests.	95. Ensure the equivalent requirements cross referencing **8.2.1** for each of the rights are consistent, using 'process' or 'respond' as appropriate. NB. This applies to **8.2.2.6, 8.2.3.6, 8.2.4.6, 8.2.5.7, 8.2.6.7, 8.2.7.3, 8.2.8.4, 8.2.9.2**.	All relevant requirements now amended to say 'process'. COMPLETE
		8.2.2, NB 4	**NB 4** outlines when privacy information doesn't have to be provided. However, there is no reference to documenting reasoning for not providing the information which would be needed in the event of a complaint or investigation, as well as demonstrating accountability.	96. Include a requirement in the control section for documenting reasons for not providing privacy information.	Control added COMPLETE 8.2.2.9
		8.2.2, data processor alternative control	**8.2.2** states that the right to be informed control does not apply to data processors, but this is not strictly true. Whilst the legal obligation is on the controller, the processor should assist the controller to apply all rights as per Article 28(3)(e). For example, this may apply where the processor is collecting information on behalf of a controller.	97. Amend the data processor alternative control to require processors to assist controllers in respect of their rights as per Article 28(3)(e). See relevant actions at **No. 104**	Amended to add 'See also 8.3.6.13 and 8.3.6.14.' for parity with other controls. PARTIALLY How this has been amended leaves **8.2.2** as the control reference, which is already the reference number of the rights section. If this is a requirement on the processor, then it needs a unique reference number. Alternatively, now **8.3.6.14** and **8.3.6.15** (was **8.3.6.13/14**) are cross referenced and are about assisting the controller re. DS

					rights, it could just say **8.2.2** doesn't apply and to see **8.3.6.14** and **8.3.6.15** as for the other rights. Update Annex 3 accordingly.
		8.2.2	There is no requirement to keep a log of historical privacy notices, including the dates of any changes, in order to allow a review of what privacy information was provided to data subjects and when.	98. Include a requirement to keep a log of historical privacy notices, including the dates and details of any changes. See accountability framework for more information.	Requirement added as new **8.2.2.6**. COMPLETE
			Our accountability framework also suggests it is good practice to review privacy notices against the ROPA to ensure it remains up to date and that it accurately explains what happens with individuals' personal data.	99. Include a requirement or recommendation that organisations periodically review their privacy notices against their records of processing.	Requirement added as new **8.2.2.7**. COMPLETE
3. **Right of access** – Do the criteria require that data subjects are given adequate access to and control of their data in line with Art 15 and require respective measures to be implemented? [Annex 2 ref. 8b., 10h.]	Partially	8.2.3	**8.2.3** contains requirements relating to the right of access.	-	-
		8.2.3.1	Cross-reference not in bold type as for other references. This also applies to This applies to **8.2.3.1, 8.2.4.1**, **8.2.5.1, 8.2.6.1, 8.2.7.1, 8.2.8.1**.	100. Put reference to **8.3.6** in bold type. NB. This applies to **8.2.3.1, 8.2.4.1**, **8.2.5.1, 8.2.6.1, 8.2.7.1, 8.2.8.1**.	Amended as recommended. COMPLETE
		8.2.3.2(f)	The right to lodge a complaint should be with the Information Commissioner not the supervisory authority.	101. Amend 'supervisory authority' to say, 'Information Commissioner'/ 'ICO'/ 'Commissioner' (decide which one as per earlier comments.)	Amended as recommended. COMPLETE
		8.2.3.3	This says, *"The Organisation SHALL verify the identity of the individual*	102. Reword this so it's clear whose identity is being verified.	Reworded 'Individual' to 'Data Subject'.

			who requests access" but it isn't clear if this is identity of the data subject or the person requesting, for example if it's a 3rd party making the request, or both.		COMPLETE
			Cross-reference not in bold type as for other references.	103. Put reference to **8.3.6.9** in bold type.	Amended. COMPLETE
		8.2.3, data processor alternative control	The data processor alternative control contains a note saying processors don't have to respond to requests but need to assist the controller. This isn't necessary as this is covered at **8.3.6.13** and **8.3.6.14** which are also cross-referenced here.	104. Remove note and just say 'also see **8.3.6.13** and **8.3.6.14**'. NB. This applies to all the corresponding notes for the other rights. (**8.2.3 – 8.2.9**)	Amended for all requirements. PARTIALLY These have been amended other than for **8.2.1** and **8.2.2** **8.2.1** will not apply to processors at all as this is about Art 12 and the controller facilitating the rights and should just say the section doesn't apply. See comment above re. **8.2.2**. In some of the processor alternative controls where the section has been amended the numbers have not been updated to reflect the new criteria. For example, at **8.2.3** it says, **8.2.3.1 – 8.2.3.7** do not apply to data processors, whereas it should say **8.2.3.1 – 8.2.3.9**. Check all and amend as necessary.
4. Do criteria adequately address the data subject's **right to rectification** of	Yes	8.2.4	**8.2.4** contains requirements relating to the right to rectification.	-	-

inaccurate/ incomplete data, and require respective measures to be implemented? (Art 16) [Annex 2 ref. 8c., 10h.]		8.2.4.4, 8.2.4.5	The last part of **8.2.4.4** and the first part of **8.2.4.5** appear to duplicate each other.	105. Remove duplication from **8.2.4.4** and **8.2.4.5** by deleting the last part of **8.2.4.4** and keeping **8.2.4.5** as a standalone requirement.	Amended. COMPLETE
5. Do criteria adequately address the data subject's **right to erasure,** and require respective measures to be implemented? (Art 17 & 19) [Annex 2 ref. 8c., 10h.]	Partially	8.2.5.2	Cross-reference to **NB 1** not in bold type as for other references.	106. Put reference to **NB 1** in bold type.	Amended. COMPLETE
		8.2.5.3	Says, '… erase Personal Data from all systems containing it…' but the 'containing it' bit doesn't really add anything.	107. Delete 'containing it' from **8.2.5.3**	Amended. COMPLETE
		8.2.5.4	The last sentence says, *"In addition, the Organisation SHALL inform the Data Subject about those recipients if the Data Subject requests it."* This would be better as a separate requirement as at **8.2.4.5**.	108. Separate out the last part of **8.2.5.4** into a standalone requirement.	Amended as recommended. PARTIALLY Data processor alternative control needs updating to reflect extra controls being added.
6. Do criteria adequately address the data subject's **right to restriction,** and require respective measures to be implemented? (Art 18 & 19) [Annex 2 ref. 8c., 10h.]	Yes	8.2.6	**8.2.6** contains requirements relating to the right to restriction. However, there doesn't appear to be a requirement reflecting Article 18(2) regarding only processing restricted data with the exception of storage, with the consent of the data subject or for the establishment of legal claims, etc.	109. Ensure **8.2.6** reflects Article 18(2).	18(2) now included as a control COMPLETE *New control at 8.2.6.8*
		8.2.6.2	**8.2.6.2** refers to the explanatory note at **NB1** for the circumstances when restriction will apply but these are actually provided at **NB3**. That said, the notes are a different order to the corresponding sections for other rights.	110. Reorder to notes in line with other rights (see comments below re. notes) and put cross-reference in bold type. Also see **no.113**.	Notes reordered (**NB 3** is now **NB 1**) and cross reference is now in bold type. COMPLETE

			Cross-reference to **NB 1** not in bold type as for other references.		
		8.2.6.3	See comment re. **8.2.5.4** re. last part being separated out.	111. See **no.108**	Amended as recommended, new requirement added as **8.2.6.4.** COMPLETE
		8.2.6.4	This refers to the request being manifestly unfounded or excessive, but this only applies to the right of access. This appears to be an error and should be referring to 'proves impossible or involves disproportionate effort', but this is already dealt with above at **8.2.6.3**.	112. Resolve duplication between **8.2.6.3** and **8.2.6.4**.	Duplicate removed COMPLETE
		8.2.6 - NB 1 and NB 4	**NB 1** and **NB 4** are essentially the same.	113. Resolve duplication in **NB 1** and **NB 4**.	NB 4 removed. COMPLETE
		8.2.6 - NB 3	**NB 3 –** see comment above. This should come first then the reference at **8.2.6.2** will be correct.	114. Make **NB 3** the first note.	Amended. COMPLETE
		8.2.6 – NB 2	**NB 2 -** This sentence doesn't make sense: "*In some cases, the Organisation may be able to lift a restriction, for example of how to restrict Processing include*". However, we believe that this should actually be about the circumstances where processing should be temporarily restricted rather than *how* it is restricted, eg when a data subject has contested the accuracy of the information.	115. Reword the sentence at **NB 2** to clarify intention of guidance note, ie circumstances where processing should be temporarily restricted.	Sentence reworded. COMPLETE

			The note that follows about notifying data subject if the restriction is lifted is necessary and should therefore be a requirement.	116. Include the note at **NB 2** about notifying the individual if the restriction is lifted as a requirement in the control section.	Relevant section from note removed, it seems to me that **8.2.6.7** lists this as a control so another isn't necessary. COMPLETE
7. Do criteria adequately address the data subject's **right to data portability** where that right applies, and require respective measures to be implemented to facilitate that? (Art 20) [Annex 2 ref. 4c., 10h.]	Yes	8.2.7.2	While this does say 'where the individual has provided data to the organisation' this aspect of data portability is often misunderstood, as is the fact this right only relates to information processed electronically – not paper records and could be reinforced in a note for the avoidance of doubt. This right is intended to allow individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.	117. Consider adding a guidance note to reiterate that data portability *only* applies to data provided by the individual and is processed by automated means.	Guidance note added as new NB 2. COMPLETE
8. Do criteria adequately address the data subject's **right to object** to processing, and require respective measures to be implemented? (Art 21) [Annex 2 ref. 10h.]	Yes	8.2.8	8.2.8 contains requirements relating to the right to object.	-	-
		8.2.8	The right to object only applies where the lawful basis is public task or legitimate interests, however 8.2.8 only refers to LI. Is the assumption that public task is not applicable to legal services? In which case this should be defined as out of scope in section 2.6, and in the lawful basis section at 8.3.4. For the avoidance of doubt a note should also be included at 8.2.8 to clarify why public task not included here, and that this right does	118. Determine if public task is in scope and update relevant requirements accordingly, including the scope section at 2.6. See no.57.	Public task added COMPLETE
				119. Add a note explaining when this right does/does not apply in the context of the processing in scope. For example, it only applies for processing based on public task or LI, but public task doesn't apply to legal service	Note added COMPLETE Note added at NB 2

			not apply to processing based on contract.	providers (if that is the case), and doesn't apply to processing based on contract.	
		8.2.8.5, 8.2.8.6	Formatting - **8.2.8.5** and **8.2.8.6** bullets are in a different font to the others.	120. Change font of **8.2.8.5** and **8.2.8.6** bullets to match the rest.	Amended. COMPLETE
		8.2.8, NB 1	This is about objecting to direct marketing being an absolute right and should be included as a requirement.	121. Include a requirement relating to the absolute right to object to marketing (including profiling); and that in the case of such an objection they must cease processing immediately and without question.	Requirement added to **8.2.8.4** and **NB 1** amended. COMPLETE
9. Do criteria adequately address the data subject's **right to not be subject to a decision based solely on automated decision making, including profiling**; or where necessary allows for human intervention, and require respective measures to be implemented? [Art 22] [Annex 2 ref. 10h.]	Yes	8.2.9	**8.2.9** contains requirements relating to the right not to be subject to automated decision making (including profiling).	-	-
			See comment above re. data processor alternative control at **no.104**.	-	Reference added COMPLETE
10. Do criteria require application of tech & org measures providing for the ability to intervene in the processing operation(s) in order to guarantee DS rights and allow corrections, erasures or	Yes	-	We couldn't locate any requirements relating to being able to intervene in the processing operations to guarantee data subject's rights and allow for corrections, restrictions, deletions, etc. Both physical and IT systems used in the processing need to allow for this	122. Include requirements that systems and processes allow organisations to intervene in the processing to facilitate data subject rights, including the ability to permanently delete data. They should also be able to intervene in the processing to carry out checks on the system	Added to 8.3.1 COMPLETE 8.3.1.20

restrictions (ie ensuring systems allow this) [Annex 2 ref. 8c., 10i.]			and for information to be permanently deleted. This also applies to being able to apply security patches/updates as necessary. See comments below re. Art 32.	or processes and apply updates and security patches. The Data Protection by Design and Default section at **8.3.1** might be the most appropriate place to include this. See also **no.183**.	
11. Do criteria require the implementation of enhanced data subject controls to facilitate self-determination and choice? [Annex 2 ref. 11b.]	Partially	8.1.4.4, 8.2.1	This is provided for in a limited way via: **8.1.4.4, NB 6** re. accuracy principle recommends a self-service portal is provided where possible. **8.2.1, NB 3 and 8.2.3, NB 2** re. allowing individuals to download their information for right of access via secure, self-service portal. Given the nature of the processing most information will be provided on the lawful basis of 'contract' and therefore there is not much 'self determination' or 'choice' involved. However, these could be included as recommendations in the controls with 'should' statements, rather than in the guidance notes. Alternatively a general requirement could be included in **8.3.6** for enabling data subjects to provide 'self-service' options where possible if it is felt this is suitable for the processing in scope.	123. Consider including a requirement in **8.3.6** for providing self-service options for individuals to exercise their rights where possible. Also consider upgrading the existing guidance notes referred to here as optional criteria in the control sections.	8.3.6.3 updated to require self - service mechanism Guidance notes in 8.1.4, 8.2.1 and 8.2.3 updated to controls PARTIALLY **8.3.6.3** adds a 'SHALL' requirement for self-service mechanism to exercise rights. **8.1.4.7** added: *"The Organisation SHOULD provide a self-service mechanism for Data Subjects to assist maintenance with personal data."* Should this rather say, '…assist with maintenance of personal data'? ***Amend** **8.2.1.13** added: *"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."*

					8.2.3.8 added: *"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."* These are the same – requirements can only appear once, therefore one should be deleted to remove duplication. The remaining one can be cross-referenced if necessary. NB. Due to additional controls being added, the Data Processor Alternative Control now needs updating to refer to **8.2.1.1 – 8.2.1.14**, or just refer to **8.2.1** as a whole.
G. General obligations of controllers and processors (Art 24 – 31) (Annex 7c)					
1. Do criteria require technical and organisational measures implementing **data protection by design.** ie. measures to ensure that data protection is considered from the outset and 'baked in' to every stage of the processing, including when determining the means of processing. [Art 25.1]	Yes	8.3.1	Data Protection by Design and Default is covered in **8.3.1**. Design from **8.3.1.1** to **8.3.1.7**.	-	-
		8.3.1.1 – 8.3.1.7	Throughout the design section it refers to embedding data protection. However, it isn't clear exactly what that means and as such would be difficult to audit. Requirements must set clear practical requirements that can be audited against. We have suggested some alternative wording based on ICO guidance for data protection by design and default. See comments below.	*See comments and actions below.*	COMPLETE

[Annex 2 ref. 10m.]		8.3.1.1	*"The organisation shall embed data protection when developing new IT systems…"*.	124. '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.' (from Policies and procedures | ICO)	Amended as recommended. COMPLETE
		8.3.1.2	*"The Organisation SHALL embed risk assessment when developing new IT systems…"*	125. Amend to say, '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.' or similar.	Amended as recommended. COMPLETE
		8.3.1.3	*"The Organisation SHALL embed data protection when developing new policies or processes…"*	126. Amend to say, '...ensure that data protection matters are considered and incorporated into new policies or processing that involve processing personal data.' or similar.	Amended as recommended. COMPLETE
		8.3.1.4	*"The Organisation SHALL embed data protection when entering into data transfer or sharing arrangements."*	127. Amend to say, '...shall, when entering into data transfer or sharing arrangements, that data protection risks are considered, addressed and documented'	Amended as recommended. COMPLETE
		8.3.1.6	Says, *"…that enable the data protection principles…"*. The principles are about how organisations must process personal data so 'enable' isn't really the right word. This should be about implementing or complying with the principles.	128. '...that enable implementation of the data protection principles...' OR '...that enable compliance with the data protection principles...'	Amended as recommended. COMPLETE

2. Do criteria require implementation of technical and organisational measures to ensure **data protection by default** in respect of the ToE? ie. to ensure only information that is necessary for the purpose of processing are processed and are only accessed by designated personnel. [Art 25.2] [Annex 2 ref. 10l.]	Yes	8.3.1.8 – 8.3.1.19	Data Protection by Design and Default is covered in **8.3.1**. Default from **8.3.1.8** to **8.3.1.19**.	No comments.	-
3. Do the criteria cover joint controller and processor obligations (where appropriate) [Art 26 and 28] [Annex 2 ref. N/A]	Partially	8.4	Joint controllers are covered in multiple places. Their obligations are set out in **8.4**. Supplier register is required at **8.4.1**; supplier status assessment required at **8.4.2** to determine whether supplier is controller, joint controller or processor; Supplier risk assessment covered at **8.4.3** to determine whether a Third Party service provider provides required data protection. Data sharing agreements are covered in **8.4.5**.	-	-
			Processor obligations are covered in the alternative controls for each section which outline which criteria apply or don't apply to them, or in	-	-

			some cases setting processor specific requirements.		
		8.4, intro, para 2	This says, *"It may also be contingent to arrangements with Third Parties that Client File data is necessarily shared"*, This appears to be an overly complicated way of saying that it might be necessary to share data.	129. Simplify wording to make it clear what is being conveyed here.	Wording simplified COMPLETE
		8.4.1, data processor alternative control	This correctly says **8.4.1** applies equally to processors. However, it then goes on to explain rules for not engaging a sub-processor with the controller's permission and directs them to **8.4.4.3** and **8.4.4.4**. As these are requirements relating to engaging a sub-processor it isn't really necessary to include the explanation as well.	130. Delete the explanatory note and just refer them to **8.4.4.3** and **8.4.4.4** as per other sections where this applies.	Amended as recommended. COMPLETE
		8.4.2.2	The wording "cooperate, on request, with the Commissioner in the performance of the Commissioner's tasks" sounds a little clunky. Also see earlier comments about 'the Commissioner' needing to be defined if it's to be used in the criteria.	131. Amend wording to say, 'cooperate with the Commissioner on request', ensuring if 'Commissioner' is going to be used it's included in the definitions as per action **no.27**.	Wording amended Information Commissioner added to definitions COMPLETE Now says, *"…cooperate with the Information Commissioner on request ~~in the performance of the Commissioner's tasks.~~"* Happy to accept this, although the last part (lined through) could be omitted.
		8.4.2	Guidance notes – correctly determining whether an organisation is a controller, processor or joint-controller is not always	132. Consider adding more guidance to help organisations identify if they are a controller/	Guidance note added as **NB 5.** COMPLETE

			straightforward. It might be helpful to either provide more guidance regarding potential difficulties and/or link to the ICO guidance.	processor/ joint-controller and link to relevant ICO guidance: Controllers and processors Controllers and processors - detailed guidance	
		8.4.2, NB 1	**NB 1** re. the Data Controller states: *"…where the purposes and means of such Processing are determined by law, the controller or the specific criteria for its nomination may be provided for by law*" doesn't quite capture s6(2) DPA 18 – it is about who has the obligation under the law to process the personal data.	133. Ensure wording accurately reflects the s.6(2) DPA 2018.	'obligation' added in line with DPA 2018 PARTIALLY Now says, *"...; where the obligations of such Processing are determined by law, the controller or the specific criteria for its nomination may be provided for by law."* This doesn't address our comment. s6(2) DPA 18 is about where the organisation that has a statutory obligation to process the data being designated a controller despite the purpose and means being determined by law. Our detailed guidance on controllers and processors says: *"Some controllers may be under a statutory obligation to process personal data. 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."*

					It might be better to utilise this wording in **8.4.2, NB 1**.
		8.4.2, NB 3, NB 4	Joint controllership guidance needs to be clear that joint controllers determine the purpose and means of processing together. They will not be joint controllers if they are processing the same data for different purposes. This also applies to the example of joint controllers at **NB 4**. These examples would also benefit from some context being provided, eg who instructed the barrister? What are they doing with the personal data? See also comments regarding **section 4.0 – definitions**.	134. Ensure **NB 3** and examples of joint controllers at **NB 4** accurately reflect the law and ICO guidance. Add more context to the examples. See also **action no.30** re. the definition of joint controllers.	NB3 and NB4 updated Examples expanded COMPLETE
		8.4.2, NB 4	**NB 4** Examples - 'Barristers' should be singular	135. Replace 'Barristers' with 'Barrister'.	Amended. COMPLETE
		8.4.2, data processor alternative control	This says all of **8.4.2** applies to processors, but it's unlikely that **8.4.2.3** would apply if they are a processor, as it's about joint-controllers.	136. Clarify if **8.4.2.3** applies to processors. If not, then state which specific controls apply.	Alternative control amended. COMPLETE
		8.4.3	It isn't explicitly clear if the supplier risk assessment is for only processors (as per current list at **2.2**) or for other controllers and joint controllers as well.	137. Clarify if this applies only to the assessment of third parties that are processors/sub-processors, or joint controllers as well.	Amended to clarify Data Processors COMPLETE
			There is no reference to consideration of how the third party assesses and	138. Include consideration of the third party's risk assessment process.	Added to due diligence checklist COMPLETE

			manages data protection risks as part of the due diligence exercise.		
			As currently worded, the third party supplying the answers to these questions or completing the suggested check list is sufficient - there's no reference to ensuring the subsequent findings are acceptable.	139. Amend to include an evaluation by the DPO/Data Protection Manager of the answers provided by the Third Party and to determine if they ensure an equivalent level of data protection is maintained when data is shared with third parties.	Amended – control 8.4.3.3 added. COMPLETE
		8.4.3.1	Related to the previous comment, **8.4.3.1** doesn't setting minimum requirements as envisaged in the **section 1** introduction which says, "*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...*"	140. Expand the requirement at **8.4.3.1** to say, 'The Organisation SHALL assess the data protection applied by any Third Party suppliers that will be processing Client File data to ensure that an equivalent level of data protection is maintained.' or similar.	Amended as recommended. COMPLETE
		8.4.3.1, 8.4.3.2	Whilst these cover the initial due diligence of third party suppliers, there is no requirement to conduct periodic audits of those suppliers as provided for in the contract at **8.4.4 (i)**.	141. Include a requirement (here or elsewhere if more appropriate) to conduct periodic audits of third parties in line with contractual requirements at **8.4.4**.	Control added COMPLETE
		8.4.3 – data processor alternative control	Says this applies equally to processors, but it would be helpful to clarify in what circumstances, ie when engaging sub-processors.	142. Amend to say, '**8.4.3** applies equally to Data Processors when engaging sub-processors'.	Amended. COMPLETE
4. Do the criteria require proof of contractual	Partially	8.4.4	**8.4.4** refers to 'data sharing relationships'. Whilst data *is* being shared, when we talk about data	143. To prevent confusion, remove reference to data sharing from the title of **8.4.4**.	Reference removed from title and appendices amended.

agreements between processors and controllers? [Annex 2 ref. 7a.]			sharing we are usually referring to controller-controller relationships as per our <u>data sharing code of practice</u>. It would be better to only refer to data sharing where this is the case. NB. Controller-controller sharing is covered in **8.4.5**.		COMPLETE
		8.4.4	**8.4.4** covers Data Processing Agreements for controller to processor relationships according to the section title. However, the processor alternative control says this applies equally to processors, so the title does not reflect the intention of **8.4.4**.	144. Rather than trying to pick out which controls would apply to processors as they are written, it would be better to keep this section dedicated to controller-processor sharing and create a new section for processor-processor sharing, covering obligations from Art 28(2) and 28(4), including the things covered in **8.4.4.3** and **8.4.4.4**. Amend intro to **8.4.4** accordingly.	New section for P-P included and additional controls as per Art 28 (2) and (4) PARTIALLY Section **8.4.4** has been subdivided into two sections: one for controller-processor and one for processor-processor. It isn't clear why the processor requirements are in the main control section rather than the 'processor alternative control' section. See similar comment re. **8.5.2.4** at **no.190**. **8.4.4.4** says that the processor-processor agreement will contain the "same clauses and obligations as laid out in **8.4.4.2**" (controller-processor agreement.) However, it won't necessarily contain the same clauses as, again, there isn't always a direct read across (eg processing on the instructions of the controller or notifying the controller of breaches).
		8.4.4 - Data processor alternative control	This states that **8.4.4** applies equally to processors. However, not certain that it can apply equally as it stands, as this section relates to controller to processor sharing and there isn't always direct read-across, eg **8.4.4.2(a)** - processing on instructions of controller.		
			The alternative control says there isn't an alternative control but then sets alternative controls at **8.4.4.3** and **8.4.4.4**.		

					The UK GDPR (Art 28(4) says that the same data protection *obligations* set out in the controller-processor agreement must be imposed on the sub-processor but not the same clauses. This ensures that the data is given equivalent protection but will not necessarily need a duplicate contract in place. Also, it's important to bear in mind that the processor seeking certification may not be working for a controller who is certified to this scheme. Which highlights the difference here that the P-P contract needs to mirror the specific contract the initial processor is bound by. Our guidance says, *"Sub-processors: you must not engage another processor (ie a sub-processor) without the controller's prior specific or general written authorisation. If authorisation is given, you must put in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between you and the controller."*

					8.4.4.5 should come after **8.4.4.3** as they are both about authorisation to engage a sub-processor. **8.4.4.4** should then follow. Suggested wording: '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.' **8.4.4.6** refers to sufficient guarantees as a separate thing. In Art 28(4) this is more about the contract providing those guarantees, ie the sub-processor is contractually bound to implement measures that ensure the processing complies with the law. The way it is currently written also doesn't make it clear who is providing those guarantees. This could just be incorporated into **8.4.4.4** or kept as a standalone requirement. In which case it should be focussed on what the processor seeking certification needs to do, ie obtain guarantees from the sub-processor that they

					have implemented the relevant technical and organisational measures to ensure their processing is compliant. This could be linked back to the due diligence checks at **8.4.3.2**. If numbers are amended, ensure any references to the relevant criteria are also amended.
		8.4.4.2	Whilst **8.4.4.2 (g)** requires the processor to assist the controller with their obligation to report breaches there is no specific requirement for them to report breaches to the controller. This is covered at **8.3.5.10** but only where the processor is being certified under this standard which will not be the case for all processors under contract to the controller.	145. Include a contractual requirement at **8.4.4.2** to report breaches to the controller including timescales.	Breach reporting requirement added COMPLETE
		8.4.4.2 (g)	**8.4.4.2(g)** says, *"… assists the controller in ensuring compliance with the obligations as concerns keeping information secure …."* Should 'the obligations' be 'their obligations'? This would make more sense.	146. Amend **8.4.4.2(g)** to say, '… assists the controller in ensuring compliance with their obligations'.	Amended. COMPLETE
5. Are controller-processor agreements subject to evaluation as part of the certification process? [Annex 2 ref. 7b.]	Yes	8.4.4.4	Requirements for the controller-processor agreements are set at **8.4.4.4**, therefore these will be audited to check they exist and what they contain. As well as any due	-	-

			diligence checks carried out as required at **8.4.3**.		
6. Do the criteria require a ROPA where appropriate? (Art. 30) [Annex 2 ref. 7f.]	Yes	8.3.3	**8.3.3 Processing Records** Sets out requirements and optional recommendations for ROPAs. Alternative processor control at **8.3.3.5** sets specific requirements for processor's ROPAs.	-	-
		8.3.3.3(c)	This says 'third countries' but international organisations are also to be included in the ROPA, as per Art 30(1)(e).	147. **8.3.3.3(c)** – amend to say 'third countries or international organisations'	Amended 8.3.3.3(e) as this appears to be what this note is referring to. COMPLETE Apologies – it was 8.3.3.3(e)
		8.3.3.3(g)	This requires a description of the technical and organisational security measures. To make it easier for organisations and avoid duplication of effort this can cross-reference other documents where the information might be held, for example an Information Security Policy.	148. We suggest adding a note that the ROPA can cross-reference other documents where information may be held.	Note added COMPLETE
		8.3.3.4	**8.3.3.4** set out what the ROPA should contain, but these items are in addition to what is required.	149. **8.3.3.4** - Amend to say 'The ROPA should **also** contain'.	Amended. COMPLETE
		8.3.3.4(b)	This refers to 'IT system' but there may be a number of systems involved in the processing.	150. **8.3.3.4(b)** - Refer to 'IT systems' plural.	Amended. COMPLETE
		8.3.3.4(d)	This will likely be covered at **8.3.3.3(c)** re. categories of data. This should also include criminal offence data, not just	151. **8.3.3.4(d)** - replace the data types at with 'the source of the data'.	Amended. COMPLETE

			special category and children's data. It is also important to understand where data came from as this has implications for data subject rights.		
				152. **8.3.3.3(c)** - add a corresponding guidance note providing examples of categories of data, for example criminal offence, special category and children's data. This could also include examples of what is meant by categories of individuals.	Guidance note with examples added COMPLETE
H. Data protection management system (information governance)					
1. Do criteria require a data protection management system (or equivalent) to be in place to demonstrate, inform, control and enforce data protection requirements? [Annex 2 ref. 10m.]	Partially	8.1	**8.1** covers 'organisational and client file governance'. Including: **8.1.1** Privacy council **8.1.2** DPO **8.1.3** Registration and cooperation **8.1.4** Principles (see comments above for this section) **8.1.5** DP Policy **8.1.6** Business Continuity Policy **8.1.7** Retention & Destruction Policy **8.3.6** covers Client Rights Management. **8.5** covers 'Monitor & Review'	-	-
		8.1.1.2	Grammar – punctuation needs amending to ensure requirement interpreted correctly.	153. **8.1.1.2** – Add comma after equivalent, ie '…or equivalent), the most senior…'	Amended. COMPLETE
		8.1.3	**8.1.3**, re registration with the ICO refers to 'UK Data Protection Authority', 'ICO', 'Information Commissioner' and 'Commissioner' within the same section. There needs to be a consistent approach, here and throughout the document. The 'ICO' is	154. **8.1.3.1** and **8.1.3.2**, say 'the ICO' as defined in **section 4**.	Amended to only say 'the ICO'. COMPLETE
				155. **8.1.3.3** - say 'with the Information Commissioner' or 'Commissioner' and define the relevant term in **section 4**.	Amended to 'Information Commissioner' and 'UK Data Protection Authority' added to Section 4 definition of ICO.

			defined as the Information Commissioner's Office in **section 4**, but there is no definition of Information Commissioner/ Commissioner. As 'ICO' is already defined, it's not necessary to include 'UK Data Protection Authority'. When referring to us as an organisation you should write the 'Information Commissioner's Office (ICO)' or 'the ICO'. When referring to our chief officer, for example when referring to their task or powers, say 'the Information Commissioner'. In terms of registration it is fine to say ICO, but for cooperation is better to refer to the Information Commissioner or Commissioner.		PARTIALLY Not necessary to include 'UK Data Protection Authority' in section 4, Definitions as this term has now been deleted from the criteria. See earlier comment re. definition of the 'Information Commissioner'.
		8.1.3.1, 8.1.3.2	**8.1.3.1** says, 'if the organisation is based in the UK'. This is not strictly the case. The key consideration is where the personal data is processed. If it is in the UK, they are subject to the Data Protection (Charges and Information) Regulations 2018. **8.1.3.2** also refers to being UK based. This requirement relates to the DPO pursuant to Art 37(7). However there is no reference to being UK based in this article.	156. **8.1.3.1** - amend to say, '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'	Amended as recommended. COMPLETE
				157. **8.1.3.2** – amend to say, 'If applicable, the organisation shall register the DPO's details with the ICO.'	Amended as recommended. COMPLETE

			It might be better to keep both wider to allow for all circumstances as per the territorial scope of the scheme at **2.5**.		
2. Do the criteria require the implementation of data protection policies? [Art 24.2] [Annex 2 ref. 10m.]	Partially	8.1.5, control objective	The control objective says, "To document and distribute a Data Protection Policy for the consumption of all employees that process Client File data." which doesn't sound right. Also, this section is about the DP Policy, but the objective doesn't state what the aim of the policy is.	158. Reword the control objective to say, '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.' Or similar.	Amended as recommended. COMPLETE
		8.1.5	We would expect policies to be signed off and reviewed at regular intervals but there are no requirements to that effect.	159. Include requirements for policies to be signed off and reviewed at regular intervals. This applies to the DP Policy but may also apply to other policies in the criteria.	Amended – control added at **8.1.5.4.** COMPLETE
		8.1.5.3	The reference to auditing employee awareness of the policy lacks a specific timeframe. Is it a one off? Is it regularly checked as part of the training?	160. Amend to include time period(s) for this.	Time period added COMPLETE
		8.1.5 – NB 1	This outlines what the DP Policy should contain. As **8.1.5.1** doesn't set minimum requirements for the policy it would be better to include these there.	161. Include the list from **NB 1** at **8.1.5.1** as minimum requirements for the data protection policy. For example, 'The Data Protection Policy shall cover the following as a minimum:..'	List from **NB 1** moved to **8.1.5.1** as recommended. COMPLETE

			Bullet point (a) is highlighted but there doesn't appear to be a reason for this.	162. Remove highlight.	Removed. COMPLETE
		8.1.7.7	**8.1.7** is about the Retention & Destruction Policy. **8.1.7.7** - The examples of data types from the Retention & Destruction Policy don't mention any statutory or regulatory retention periods applicable. For example, HMRC or Solicitors Regulation Authority retention rules.	163. Include reference to any statutory retention periods. A guidance note could be added to consider these when determining retention periods.	Guidance added COMPLETE
		8.1.7, data processor alternative control	This says **8.1.7** applies to processors equally, but there is a note about processors being expected to return/delete information in line with their contract. As this is the case, it should probably be an additional requirement on processors.	164. We recommend including the note as a requirement for processors to include this scenario in their policy, unless requirements are set elsewhere (see comment re. **8.1.4.5** and action **no.50**) for information to be deleted in line with the R&D policy. In which case an alternative control could be included there for processors to return/delete information as specified in their contract.	Processor guidance modified and cross referenced to 8.4.4.2 COMPLETE
		8.3.6	**8.3.6** includes requirements for managing the data subject rights process. This stands alone from the Client rights section.	-	-
			See earlier comment regarding the rights being for any data subject not only the client. Therefore the title and wording of this section needs amending to reflect that.	165. **See no.80**	Amended – see note for no.80. COMPLETE

		8.3.6.1	As for **8.3.5.1** this doesn't specify if this means published internally or externally. Is this an internal process for staff to follow or the public process for data subjects to follow?	166. **8.3.6.1** – clarify whether this process is for internal of external use and publish accordingly.	Amended to 'internal' COMPLETE
		8.3.6.3	The wording here is a bit overcomplicated, ie *"…provide a mechanism for Clients to communicate their desire to invoke a data protection right."*	167. **8.3.6.3** – reword to say, '…provide a mechanism for individuals to exercise their data protection rights.'	Amended with Data Subject instead of Individual. COMPLETE
		8.3.6.4	Again wording can be simplified here.	168. **8.3.6.4** – replace 'include the ability for' with 'enable'.	Amended. COMPLETE
		8.3.6.7	Grammar – this sentence needs breaking up for readability.	169. Include some punctuation to break up this sentence.	Commas added. COMPLETE
		8.3.6.9	Grammar – errant full-stop after ID.	170. Remove full-stop after ID.	Removed. COMPLETE
		8.3.6.10	This relates to the register at **8.3.6.8** so should follow it.	171. **8.3.6.10** should immediately follow **8.3.6.8** introducing the register.	**8.3.6.10** amended to **8.3.6.9**. COMPLETE
		8.3.6.12	Cross-reference not in bold type.	172. Make reference to **8.2.1** bold.	Amended. COMPLETE
		8.3.6.14	This sets a requirement where the processor is contacted by the data subject. However, **8.3.6.13** already requires the processor to direct the DS to the controller where that happens.	173. **8.3.6.14** - This should just be about assisting the controller - not if it's contacted by the DS, ie, 'The data processor shall assist the data controller in respect of the request as required.' (or similar).	Amended to remove reference to Data Subject contact. COMPLETE

		8.3.6, NB 2	Not clear if this means the right of access specifically or rights requests as a whole.	174. Clarify what request this is referring to.	Text clarified COMPLETE
			Refers to training including a reference to this process, but this could be worded a more clearly.	175. Reword to say, 'training should cover the rights management process.'	Amended. COMPLETE
		8.3.6, NB 3	This goes further than an explanatory note and reads as a requirement.	176. We recommend that meeting regularly to discuss progress on rights requests should be included as a requirement, or at the very least as a recommendation in the control section.	Changed to a control PARTIALLY **8.3.6.13** added. Data processor control needs amending to reflect addition of **8.3.6.13**. Only refers to **8.3.6.1 – 8.3.6.12**.
3. Do criteria require measures providing for **transparency** of processing operations with respect to: i. Accountability? ii. Data subjects rights? iii. Assessment of individual processing operations, e.g. for algorithmic transparency? [Annex 2 ref. 10m.]	Yes	8.1, 8.2, 8.3, 8.5	Transparency is covered in the following sections: **8.1.4** re. the first principle. **8.2** re. right to be informed and providing clear information about the processing, including re. automated decision making. **8.4.5** re. data sharing. **8.4.6** re. international transfers. Accountability re. transparency: **8.5.2** – review of privacy notices. **8.3.4.5** – record of privacy info provided at time of obtaining consent. No register/log of privacy notices. See comment re. **8.2.2** and action **no.98**.	177. Ensure the approach to transparency generally reflects the accountability framework.	98 and 99 actioned COMPLETE Training guidance updated COMPLETE 8.1 amended COMPLETE 8.1.1.3 added re. transparency of processing. DPIA control added COMPLETE 8.3.2.14 added re. publishing DPIAs.

			Our accountability framework also recommends periodically reviewing privacy information against the ROPA to ensure people are being given the right information. See action **no.99** There is also a need to educate staff and third party suppliers where appropriate of the need to provide privacy information, in particular front-line staff, but this is not covered at **8.3.6** re. client rights management or in **8.3.9** re. DP training. See action **no.182** below. There is no reference to a general approach transparency in the governance section at **8.1**. This could perhaps go include a requirement for maintaining a transparent approach to data processing and ensuring compliance with transparency obligations. Publishing DPIAs (or a summary of) is also a way of being more transparent about the processing in particular the associated risks and how they have been addressed.		
4. Do criteria require technical and organisational measures to ensure personnel with regular access to personal data receive appropriate periodic **training**? [Annex 2 ref. 10n.]	Yes	8.3.9	This section refers to data protection training but doesn't explicitly talk about who is being trained. Whilst it should go without saying that the requirements in this section relate to training of staff and other people handling personal data within the organisation, it is better to be explicit.	178. Ensure requirements in **8.3.9** refer to training of staff (and others, eg contractors - as appropriate to the processing), at least for the initial requirement at **8.3.9.1**.	**8.3.9.1** amended and first part of **NB 1** removed. COMPLETE

			This is covered in the guidance notes but not in the requirements.		
			The description of the data protection training is covered at **NB 1** but there is no indication of who should provide the training or to what level staff should be trained. One of the DPO's tasks (included at **8.1.2.5**) is to provide/oversee data protection training which isn't reflected in **8.3.9**. Our accountability framework section on Training and awareness sets out our expectations for training, including regular review of training and sign-off by senior management.	179. Include requirements that responsibility is assigned for managing data protection training, that there are dedicated and trained resources available to deliver training to all staff (this can be internal or external), that the training programme is regularly reviewed and signed off by senior management.	Additional controls added COMPLETE
		8.3.9.4	This requires attendance to be monitored by the DPO or equivalent. However, the monitoring may need to be wider to ensure training is monitored appropriately.	180. Amend wording to say, 'the organisation shall keep training records which shall be monitored to ensure all staff receive and complete DP training…' or similar.	Amended as recommended. COMPLETE
		8.3.9.6	This requirement relates to onboarding (presumably of staff) but comes after refresher training. It would make more sense for this to come first.	181. As **8.3.9.6** is about initial training, put it before **8.3.9.5** about subsequent periodic training. Also make it clear this is about the staff onboarding process.	Amended as recommended. COMPLETE
		8.3.9 - NB 1	This states what subjects should be included in the training, ie: a) Definition of Personal Data	182. Include the requirement to train staff (and others as appropriate) on the need to provide privacy information, in	Guidance modified COMPLETE

			b) Core areas of Client data Processing c) Sharing Client data with others d) What to do when there is a Data Breach e) What to do when I receive a rights request from a Client f) Working Remotely g) Disposing of Client data But this doesn't include training on the need to provide privacy information to clients and other individuals whose data is being processed, in particular to frontline staff.	particular to frontline staff. See accountability framework for more information.	
5. Do criteria require measures providing for the ability to intervene into the processing operation in order to patch or check the system or the process? [Annex 2 ref. 10j.]	Yes	8.3.7.2	This refers to a procedure for applying patches and updates. However, there is no reference to being able to intervene in the processing to apply patches or carry out checks on the system or processes. Without the capability it would not be possible to apply patches and updates. This relates to our earlier comment re. applying data subject rights.	183. Ensure there is a requirement to be able to intervene in the processing to apply patches or carry out checks on the system or processes. See action **no.122.**	Requirement added COMPLETE 8.3.1.20
6. Do criteria require **self-assessment/ internal audit**? [Annex 2 ref. 10p.]	Yes	8.5	8.5 contains requirements relating to monitoring their compliance against the controls. It includes: 8.5.1 – Internal Audit Process 8.5.2 – Internal Audit review	-	-
		8.5.1, NB 1	Not clear what is meant by 'LOCS format'. Does it mean the LOCS Standard format, ie the controls?	184. Clarify what is meant by 'LOCS format'	Reworded to LOCS:22 Standard. COMPLETE

					"LOCS:23 Standard"
7. Do criteria require review and updating of the organisation's technical and organisational measures to ensure their effectiveness? (Art 24.1) [Annex 2 ref. 7d., 10o., 10s.]	Partially	8.5.2	**8.5.2** contains requirements to review and update the measures implemented to comply with the standard.	-	-
		8.5.2.1	**8.5.2.1** says the organisation shall 'have' a documented review.	185. Reword to say they shall 'undertake an annual review and document their findings and recommendations.'	Amended as recommended. PARTIALLY Acknowledge this uses the suggested wording, but now it's not clear what is being reviewed. Amend to say, 'undertake an annual review of their data protection measures and document their findings and recommendations'; or 'undertake an annual data protection audit and document their findings and recommendations.' (in line with wording of **8.5.2.2/3**)
		8.5.2.3 (c)	Point 'l' says 'website privacy notice (**8.2.2**)' however, this won't always be on the website. There may be other privacy info provided, eg on forms completed, additional consent requests, just-in-time notices which is also reflected in **8.2.2**.	186. **8.5.2.3 (c)** - Amend wording here to reflect that - eg privacy notices/privacy information.	Amended to say 'Privacy Notices'. COMPLETE
		8.5.2.3 (d)	This states what documentation should be audited for storage limitation, ie retention schedule and retention policy. However, they should also audit effectiveness of those policies by sampling data - is	187. **8.5.2.3 (d)** - Amend to include checking effectiveness of policies and procedures	Text amended PARTIALLY Wording amended but doesn't quite make sense, ie "The Organisation should ensure that

			data being weeded in line with the retention schedule and destroyed properly?		existing policies and schedules are effective, up to date and periodic spot checks that each that each business area is actively meeting requirements". What is happening re. spot checks? Should this say spot checks are undertaken to ensure each business area is adhering to the relevant policies/procedures? As this is not just about auditing documentation it would be better to reword "Key documentation to be audited are:" to reflect that.
		8.5.2.3 (e)	This refers to the Transfer Impact Assessment (TIA), however note comments below re. aligning wording with ICO guidance.	188. **8.5.2.3 (e)** - If wording is changed to Transfer risk Assessment (TRA) then amend here also. See action **no.224.**	Added 'effective' before 'up to date'. (NB. Think this comment relates to previous recommendation.) COMPLETE Amended to say Transfer Risk Assessment.
		8.5.2.3 (f)	This is headed 'IT Security', but all security measures should be audited including physical security. This is actually reflected in the list provided here but not in the heading.	189. **8.5.2.3 (f)** – Amend heading to say 'security'.	Amended. COMPLETE
		8.5.2, Data processor alternative control	This states **8.5.2** applies equally to data processors, however not all of the controls in **8.5.2** are applicable to processors. For example, c) Privacy	190. May need a complementary requirement for processors that replaces **8.5.2.3**.	Amended to reflect Data Processor requirements PARTIALLY

			policies - stated as not applying to processors (which is correct); and e) data sharing - no reference to processor-processor sharing. (See earlier comments regarding this.)		This should rather be in the 'data processor alternative control' section rather than in the main control section as it only applies to processors. Our understanding is that this section is for setting processor specific requirements as necessary - either instead of or in addition to the main controls. See similar comment re. **8.4.4** at **no.144.**
I. Security (Art 5(f), Art 32)					
1. Do criteria require technical and organisational measures to ensure **confidentiality** of processing operations? (To protect personal data from inappropriate disclosure) [Annex 2 ref. 10a.]	Partially	8.3.7, 8.3.8	Technical security measures are covered in **8.3.7** and organisational measures in **8.3.8**.	-	-
			There is no reference in either section on security about the need to have an information security policy. Neither is this specifically mentioned in **8.1.5** Data Protection Policy, although it does say it should cover elements related to security such as 'how data is protected'. It is however referred to in **8.3.3, NB 2** re. linking to the information security policy in the ROPA.	191. Consider whether it would be appropriate (depending on the size of organisations in scope) to include a requirement or recommendation for an Information Security Policy. For example, 'Unless information security is explicitly covered the data protection policy, the organisation shall implement an Information Security Policy covering the following subjects…' Amend the reference at **8.3.3, NB 2** accordingly.	Requirement for InfoSec Policy added 8.3.3 NB 2 cross referenced COMPLETE Requirement for InfoSec policy added at 8.1.5.2 and cross-referenced at **8.3.3, NB 2.**

		8.3.7.1	**8.3.7.1** says organisations must document the core business systems in a system map. Presumably this would only be the core business systems involved in the processing?	192. Clarify if these are the core business systems involved in the processing.	Clarified PARTIALLY This now says, "systems that involve Personal Data processing". Would *all* the systems involved in the processing being certified *always* involve personal data? And would all systems that process personal data relate to the Client File? Perhaps might be better to amend this slightly. For example, 'An Organisation SHALL document the core business systems processing in a Systems Map, clearly identifying those that process Client File data.' This would tie in with other requirements in this section, eg **8.3.7.2** and **8.3.7.12**.
		8.3.7.3	This says organisations must apply security patches immediately 'on receipt' but would they always be receiving them from someone/somewhere?	193. Consider amending wording to say '…immediately when they become available.'	Amended as recommended. COMPLETE
		8.3.7.13 and NB 8	**NB 8** says the biggest risk to breach of client file data is human error. Which we would agree with. However, **8.3.7.13** relating to this is only a recommendation not a requirement.	194. If this is the biggest risk related to the processing, then **8.3.7.13** should rather be a requirement than a recommendation.	Amended from SHOULD to SHALL. COMPLETE *Now 8.3.7.16*
		8.3.8.7	This only recommends that hard copy data be locked away at the end of	195. Make **8.3.8.7** a requirement to ensure hard copy	Amended from SHOULD to SHALL.

			each day, yet this poses a significant security risk.	information is protected in line with **8.3.8.8.**	COMPLETE
2. Do criteria require technical and organisational measures to ensure **integrity** of processing operations? (Ensuring accuracy and consistency of data over its entire life-cycle) [Annex 2 ref. 10b.]	Yes	-	Accuracy is only covered at a very high level in **8.1.4.4**. There are no requirements for ensuring accuracy, consistency, and completeness over the lifecycle of the processing. See our comments for **8.1.4.4** and related required actions.	196. Ensure there are requirements ensuring accuracy, consistency, and completeness of data over the lifecycle of the processing. Also see **no.49**	Requirement added and cross referenced COMPLETE Requirement added at **8.3.7.12** and note at **NB 8** referencing testing data and **8.1.4.6** re. checking accuracy.
3. Do criteria require technical and organisational measures to ensure **availability** of processing operations? (Ensuring that data continues to be available at a required level of performance in all circumstances (business continuity)) [Annex 2 ref. 10c.]	Yes	8.1.6	A 'Business Continuity Plan' is required at 8.1.6 This section uses the term 'Business Continuity Plan' throughout, but **NB 2** and the title of the section refer to 'Business Continuity Policy'.	197. Amend heading of **8.1.6** and **NB 2** to say 'Business Continuity Plan' for consistency.	Amended. COMPLETE
4. Do criteria require the application of TOMs to ensure data minimisation, for example, unlinking or separation of the data from the data subject, anonymisation or pseudonymisation, or isolation of systems? [Annex 2 ref. 10k.]	Partially		Data minimisation and pseudonymisation are covered in the DP by Design and Default section ay **8.3.1**. Data minimisation is covered at a high level in the principles section (**8.1.4.3**). Anonymisation is not mentioned at all. There isn't any reference to using data minimisation in relation to security, although **8.1.7.9, NB 2** re. archiving	198. Include security-specific requirements using data minimisation, for example, unlinking or separation of the data from the data subject, anonymisation or pseudonymisation, or isolation of systems insofar as they relate to the processing in scope. See our Security guidance for more information.	Anonymisation, pseudonymisation requirements added and cross referenced to data minimisation PARTIALLY Requirements added for Anonymisation: **8.3.7.17** Pseudonymisation: **8.3.7.18**

			refers to the possibility of moving data to an archiving system. There are possibly more measures that could be implemented to protect personal data. For example, when a client engagement is finished, but information still needs to be retained – consider if the file could be weeded and duplicate/unnecessary info deleted before being pseudonymised and moved to a separate system.		Notes link these to assisting with meeting data minimisation principle. Note at **NB 18** refers to applying **8.3.7.15** and/or **8.3.7.16** but should this be **8.3.7.17** and **8.3.7.18**?
5. Do criteria include requirements for encryption? [Art 32(1)a] [Annex 2 ref. N/A]	Partially		Encryption is required at **8.3.7.9** for removeable devices. **8.3.7.6** requires backup data to be encrypted. **8.3.6, NB 4(j)** requires the DPO to provide information to a DS via secure method such as encrypted memory stick. There are no requirements for a general approach to encryption, including when or how or minimum standards.	199. Include more general requirements relating to the use of encryption reflecting Article 32(1)(a) and in line with our guidance on Encryption.	General requirement added at 8.3.7.9 PARTIALLY **8.3.7.9 -8.3.7.11** added re. use of encryption. **8.3.7.9** says, *"The policy SHALL include appropriate staff training"*. Not clear what this means. Is it that it should include details of what training should be provided to staff re. how/when to encrypt data? *Make requirement more specific.
J. Notification of personal data breaches (Art 33 & 34)					
1. Do criteria require measures to ensure that **personal data breaches** are notified where required and in due time (to the ICO and to data subjects)? [Annex 2 ref. 10q.]	Partially	8.3.5.3	Refers to 'material' breaches but doesn't explain what this means. However, this is explained at **NB 2**.	200. **8.3.5.3** - Cross reference NB 2 where a material breach is defined.	Amended. COMPLETE
			This states that organisation must report material breaches within 72 hours. Is the expectation that this happens 100% of the time? Art 33(1)	201. **8.3.5.3 -** Cross reference **NB 2** where a material breach is defined.	Amended. PARTIALLY

			allows for situations where this hasn't been possible - but reasons for delay must be reported. This also doesn't specify that it is reportable within 72 hours of becoming aware of the breach.		Apologies – the wrong recommendation appears to have been included here which doesn't match the comments and duplicates no.200. **8.3.5.3** needs to specify that the breach needs to be reported to the ICO within 72 hours of the organisation becoming aware of it. Also consider whether the organisation must always report within 72 hours in line with our comment.
		8.3.5.4	Refers to 'high risk personal data breach but doesn't explain what this is. However, this is explained at **NB 3**.	202. **8.3.5.4** - Cross reference NB 3 where a 'high risk' breach is defined.	Amended. COMPLETE
		8.3.5.5	This refers to 'internal data breaches' but it isn't clear what that means. Article 33(5) says to document 'any' breaches.	203. **8.3.5.5** – delete the word 'internal'.	Amended. COMPLETE
		8.3.5.6	The statement at 8.3.5.6(g) and (h) don't fit with the opening sentence for the list.	204. **8.3.5.6(g) and (h)** - To fit with the opening sentence these should say, 'description of'.	Amended. COMPLETE
		8.3.5.8	This sets requirements for what information should be reported to the ICO. However, it doesn't cover circumstances where it is not possible to provide all the information at once, for example where the breach is still under investigation.	205. Include a corresponding guidance note regarding when all information is not yet available, as per Art 33(4) and our guidance Personal data breaches	Guidance note added COMPLETE Added at NB 3

		8.3.5.9	This doesn't appear to cover circumstances where the organisation doesn't have to report it to the DS, as per Art 43(3). **NB 3** covers when a breach should be reported to a client but not where it isn't necessary.	206. Ensure the circumstances where the affected parties don't need to be notified, pursuant to Art 43(3) are reflected in the requirements and/or notes as appropriate.	34 (3) is now reflected in the control and guidance PARTIALLY Requirement added at **8.3.5.10** and corresponding note explaining circumstances at **NB 5**. Check if alternative processor control needs updating to reflect addition of **8.3.5.10**.
		8.3.5.9, NB 3, and NB 6	These refer to reporting a breach to a client. However, a breach may affect more than just the client, eg if a file is lost containing 3rd party information.	207. Ensure the whole section at **8.3.5** reflects the fact that a breach could affect people other than the client.	Wording altered, mostly rewording 'Client' to 'Data Subject' to better reflect ICO recommendations. COMPLETE
		8.3.5.9, NB 2	As above – this is just about risks to the client and doesn't consider others who may be affected.	208. See **no.207**	See above. COMPLETE
2. Do criteria require incident management procedures to be in place and verified? [Annex 2 ref. 10r.]	Yes	8.3.5.1	This says the organisation must have a published process for breach reporting but doesn't specify if this is internally or externally.	209. **8.3.5.1** – clarify if organisations must publish the breach reporting process internally or externally.	Clarified as internally COMPLETE
K. Data Protection Impact Assessment (Art 35-36)					
1. Do the criteria require an assessment of the risk and the impact of the processing to the rights and freedoms of natural	Partially	8.3.2	Covered in **8.3.2 - Risks and Data Protection Impact Assessment (DPIA)**.	-	-
		8.3.2, intro	This section is about the initial assessment of risk and DPIAs but talks	210. Amend introduction to refer to general/initial assessment of	Introduction amended

persons (including a DPIA where required)? (Art 35) [Annex 2 ref. 9a., 9c.]			about DPIAs first, whereas the initial assessment would precede the DPIA, and indeed determine whether a DPIA is even necessary.	data protection risks before talking about DPIAs.	COMPLETE
			2nd para says, "In the event a DPIA is not required it is recommended that the reasons a DPIA has been ruled out is documented and an initial risk assessment be carried out in any case.", however this is now a requirement at 8.3.2.4 and precedes the DPIA so the intro should reflect that.		
		8.3.2.4	Reference to **NB 1** not in bold.	211. Make reference to **NB 1** bold.	Amended. COMPLETE
		8.3.2.10	This refers to 'data protection impact assessment' but preceding requirement use the acronym, 'DPIA'.	212. Use the acronym instead of the full term as this has already been defined.	Amended. COMPLETE
		8.3.2.13	The wording of this could be misinterpreted. It can be read as 'annually or sooner only if the risk changes', or 'annually, but sooner if the risk changes.'	213. Insert a comma after annually to separate the two circumstances where the DPIA should be reviewed.	Amended. COMPLETE
		8.3.2, NB 1	This explains how the 'short form DPIA' (initial assessment) works and provides a list of questions to be considered. However there is no reference to considering the risks based on the answers to these questions.	214. Include consideration of the risks arising from the list of questions in the short form DPIA.	Text modified PARTIALLY Text amended but typo in brackets – says, 'oe' instead of 'or'.

		8.3.2.14	This is an alternative control for data processors, requiring them to 'carry out risk assessments as appropriate'. However this is non-specific language and needs to be defined.	215. To ensure this can be audited we suggest one of two options: **a)** Processors could be required to have some form of risk assessment process in place and therefore some of the requirements here could apply, eg **8.3.2.1 - 8.3.2.5** (excluding the DPIA requirement in **8.3.2.4 - 5**); or **b) 8.3.2.14** could be amended to say, 'An Organisation SHALL have a process in place to identify, document, mitigate and manage information risks.' Option **b)** may be the most straightforward.	Amended in line with recommendation option b. PARTIALLY Two alternative requirements included for processors in line with option b). However, statement at beginning says *"**8.3.2.5 – 8.3.2.13** do not apply to Data Processors."* But these now go up to **8.3.2.14** so needs amending. This applies elsewhere – see comments in relevant sections.
		8.3.2, Data Processor alternative control	Data Processor alternative control states that there is no obligation for a Data Processor to complete a DPIA. However, there is a requirement in Article 28 for a processor to assist the controller with completion of a DPIA.	216. Include an alternative control for processors to assist controllers with their DPIA as required.	Added **8.3.2.15**. COMPLETE
2. Do the criteria provide or require a recognised risk assessment methodology? If appropriate, is it commensurate? [Annex 2 ref. 9b.]	Yes	-	Does not set a specific methodology, this is left to the organisation to determine. However, sufficient requirements and guidance are included to ensure risks are considered fully, including where a DPIA is not legally required.	-	-
3. Do the criteria, require prior consultation concerning the remaining	Yes	8.3.2.9	Yes – at **8.3.2.9**. No amendments required.	-	-

risks that could not be mitigated, based on the results of the DPIA? (Art 36) [Annex 2 ref. 9d.]					
L. Data Protection Officer (Art 37-39)					
1. Do the criteria incl. the requirement to assess need for DPO? (Art 37.1) (Including documenting decision where one isn't appointed.) [Annex 2 ref. 7e.]	Partially	8.1.2	This section refers to 'large scale' processing, but this is not defined anywhere in the document. It would be helpful to add a guidance note here or add a definition in **section 4.0**.	217. **8.1.2.1(b)** – add a note to define what is meant by 'large scale' or include a definition in **section 4.0**. Although not defined, there are some examples of large scale processing in our DPIA guidance When do we need to do a DPIA? | ICO See action **no.26.**	Definition added with link to ICO guidance COMPLETE Added note at NB3 and definition.
		8.1.2.3	In the absence of a DPO this requires the organisation to appoint an 'alternative manager of data protection'. Our Accountability Framework says, "If your organisation is not required to appoint a DPO, you appropriately assign responsibility for data protection compliance and you have enough staff and resources to manage your obligations under data protection law." This is about making sure that responsibility is assigned, but this could be one person, multiple people, or a designated 'committee', depending on the size and structure of the organisation. It doesn't necessarily need to be a 'manager'.	218. Consider if this necessarily needs to be a 'manager' of data protection or if it could be reworded to allow for alternative solutions. If this requirement is reworded amend the note at **NB 1** accordingly.	NB 4 added to include wider options PARTIALLY **8.1.2.3** amended as well as **NB 4** being added. Wording of **8.1.2.3** doesn't really work, ie *"…or appoint an alternative responsibility for…"* Suggest amending to, 'or assign alternative responsibility for…'

2. Where relevant do the criteria set out DPO requirements? (Art 37 – 39) [Annex 2 ref. 7e.]	Partially	8.1.2.5 (d)	This includes requirements for the DPO 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 to other domestic law relating to data protection (e.g. PECR)".* PECR sits alongside data protection legislation but relates to electronic marketing. However, PECR also applies even if organisations are not processing personal data.	219. So that there is no confusion that PECR is also a data protection law we suggest amending the wording to say, '…the UK GDPR and other relevant laws, such as PECR'.	Amended. PARTIALLY Wording amended. However, just noticed that bullet points of **8.1.2.5** start at 'd' instead of 'a'. *Amend
		8.1.2.5(i)	This refers to prior consultation – presumably for DPIAs although this isn't stated. Also this is doesn't cross-reference the relevant criteria.	220. Clarify if this is prior consultation for DPIAs, in which case cross-reference **8.3.2.9.**	Clarified and cross referenced COMPLETE (See note above re. amending bullet points)
M. Transfers of personal data to third countries/international organisations (Art 44 – 49)					
Do the criteria cover requirements to ensure lawful transfers of data to third countries, including adequacy, appropriate safeguards, binding corporate rules, derogations? **(excluding 46(2)(e) and (f))** [Annex 2 ref. N/A]	Partially	8.4.6	Requirements for international transfers are covered in the data sharing section at **8.4.6**. However there is some confusion in this section and the Chapter V of the UK GDPR is not accurately reflected. See comments below.	-	-
		8.4.6 - heading	The section heading refers to transfers outside of EEA, but UK GDPR only applies to the UK.	221. Delete reference to EEA from the section heading at **8.4.6**.	Deleted. COMPLETE
		8.4.6, Intro, para 2	This refers to 'UK safeguards' being identified. This appears to bundle up the 'safeguards' are from Art 46 and adequacy regulations. However, if	222. This should be reworded to say, 'This means that if it is necessary to process Client File Personal Data outside of the	Reworded as recommended. PARTIALLY

			adequacy regulations are in place, then no safeguards are necessary. This is because If adequacy regulations are in place, it's not a restricted transfer (see comment below). Adequacy is not a 'safeguard' in itself.	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.' or similar.	Suggested wording used however, the apostrophe before 'This' has been pasted by accident and needs deleting.
		8.4.6	Although the term restricted transfer is used in this section an explanation of what that means is not included.	223. Include an explanation of what is meant by a restricted transfer.	Added to definitions PARTIALLY Definition added. However, it says, "legally distinct from the exporting Organisation (receivers)" which makes it sound like the exporting organisation is the receiver which is not the case. The term 'receiver' isn't used in **8.4.6** so not necessary to include. Suggest rewording to say, 'means a transfer of personal data to a separate controller or processor located outside the UK, who is legally distinct from the exporting Organisation.'
		8.4.6	Note the ICO uses the term transfer risk assessment (TRA) rather than Transfer Impact Assessment (TIA) used in this scheme.	224. To avoid confusion, consider aligning terminology to ICO guidance to avoid confusion and refer to a transfer risk assessment (TRA).	Aligned to TRA COMPLETE
		8.4.6.1	This requires a transfer impact assessment before making a restricted transfer. However, in this section this	225. The requirement to do a TRA/TIA should come after checking to see if an	Control added Guidance note added

			is also taken to include where adequacy regulations are in place. However, our newly published transfer risk assessment (TRA) guidance says: 'You need to carry out a TRA if you are making a restricted transfer and you wish to rely on one of the Article 46 transfer mechanisms, such as the IDTA, Addendum or BCRs. You do not need to carry out a TRA if you are making a transfer to any country covered by UK adequacy regulations or if the transfer is covered by one of the exceptions.' Therefore consideration of adequacy should come before the requirement to carry out a TRA. NB. we also have a TRA tool that organisations can use.	organisation is covered by adequacy regulations. Where that is the case the transfer can take place with no further action.	Link to TRA tool added COMPLETE Control added at 8.4.6.1.
		8.4.6.2	This sets requirements for what a TIA should comprise. However, these questions don't address the risks associated with the transfer. Neither do they entirely align to the questions in our TRA, ie: **Question 1:** What are the specific circumstances of the restricted transfer? **Question 2:** What is the level of risk to people in the personal information you are transferring? **Question 3:** What is a reasonable and proportionate level of investigation,	226. The requirements at **8.4.6.2** should be expanded to include questions about current risk and whether there is an increased risk from the transfer.	Questions added COMPLETE

			given the overall risk level in the personal information and the nature of your organisation? **Question 4:** Is the transfer significantly increasing the risk for people of a human rights breach in the destination country? **Question 5:** (a) Are you satisfied that both you and the people the information is about will be able to enforce the Article 46 transfer mechanism against the importer in the UK? (b) If enforcement action outside the UK may be needed: Are you satisfied that you and the people the information is about will be able to enforce the Article 46 transfer mechanism in the destination country (or elsewhere)? **Question 6:** Do any of the exceptions to the restricted transfer rules apply to the "significant risk data"? The "significant risk data" is the data you identify in Questions 4 and 5 as data which your Article 46 transfer mechanism does not provide all the appropriate safeguards for.		
		8.4.6.3 (a)	This refers to adequacy regulations being one of the safeguards which is not the case. The safeguards are as outlined in Art 46, eg BCRs, SCCs, etc.	227. As per comments above – the consideration of adequacy should come first, before the TRA.	Adequacy removed as a safeguard and added as initial control PARTIALLY Control for adequacy added at **8.4.6.1** and removed from safeguards at **8.4.6.4**. However the introductory sentence at

					8.4.6.4 should be amended to reflect the fact this is when not relying on adequacy. Eg, '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'.
		8.4.6.3 (b) and (c)	These refer to the '2018 Act' rather than the 'DPA 2018'.	228. Refer to DPA 2018 or DPA 18.	Amended. COMPLETE
		8.4.6.3 (c)	This is an international data transfer agreement (IDTA) in the UK. See International data transfer agreement and guidance | ICO	229. Refer to the international data transfer agreement (IDTA) issued by the Commissioner.	Refers to IDTA and link in guidance COMPLETE
		8.4.6.4	Wording – "…shall be made transparent to the client."	230. It would be better to say, 'communicated to the client'.	Amended. COMPLETE
		8.4.6, NB 3	This says, *"This is an area that is currently under revision by the ICO…"* which was fair to say at the time of drafting. However, we have issued more up to date guidance in the time this document has been developed that are relevant here, including IDTAs, the TRA guidance and TRA tool referred to above.	231. Update **NB 3** to reflect the current position of ICO guidance on international transfers, including IDTAs and TRAs. Provide links as required.	Guidance notes updated COMPLETE
		8.4.6, Data processor alternative control	This says **8.4.6.1 - 8.4.6.5** do not apply to processors. However if they are making an international transfer with the permission of the controller they would apply. Note our guidance re. TRAs which says, "If you are a controller, and your	232. Add another requirement after **8.4.6.6** saying if agreed by controller then section **8.4.6** applies.	Requirement added at **8.4.6.8.** PARTIALLY Initial statement is that **8.4.6.1 – 8.4.6.6** do not apply to processors. But if they have permission of the controller as per **8.4.6.7** then they do as per

			processor is making the restricted transfer, only the processor must complete the TRA. Please see our guidance on International Transfers to determine whether it is the controller or processor that is responsible for making a restricted transfer." It goes on to say, "In that situation, you must still carry out reasonable and proportionate checks about whether the processor's restricted transfers are compliant with UK GDPR, including its obligation to carry out a TRA. This is part of your obligation to ensure your processor provides you with "sufficient guarantees" in Art 28 UK GDPR. You may also need this to assist you in demonstrating you have a lawful basis under Article 6 UK GDPR for processing carried out by the processor on your behalf."		**8.4.6.8**. Therefore, might be better to make that clear in the initial statement, eg '**8.4.6.1 – 8.4.6.6** do not apply to Data Processors unless the following apply..' or similar.'
		8.4.7	**8.4.7** covers legal service providers not located in the UK. Although technically this relates to Article 27, not international transfers, we are including comments about that here as it is included in the international transfers section of the standard.	-	-
		8.4.7 - Control Application Guidance	The note at **NB 1** uses the wording from Article 27(2)(a), and formats it into a list in an endeavour to make it clearer. However, in doing so the meaning of the Article is lost.	233. Amend wording to accurately reflect Article 27(2)(a).	Amended to remove list format and add reference for criminal offence data. COMPLETE

			For example c) refers to processing criminal offence data instead of NOT processing it. And ALL these points must be true, not each on their own.		
		8.4.7 - Data processor alternative control	This refers organisations to **8.4.4.3** and **8.4.4.4** which relate to engaging sub-processors and the relevant agreements. It isn't clear how these are relevant.	234. Clarify if **8.4.4.3** and **8.4.4.4** are relevant.	Reference to 8.4.4.3 and 8.4.4.4 removed COMPLETE
N. Criteria for the purpose of demonstrating the existence of appropriate safeguards for transfer of personal data in the meaning of Article 42(2) where the certification is intended to act as transfer tool in itself.					
N/A					
O. Other					
Cover page	n/a	p.1	As 22 denotes the year – there is a question whether this will still be the LOCS:22 Standard by the time it's formally approved. Would it perhaps be better to have a version number rather than the date? Or this information could be included on a second page before the Contents page, with the copyright information. (As per ADISA Standard)	235. Consider whether the acronym for the standard should include the number denoting the year, and include some kind of version control at the beginning of the document.	Year changed to reflect launch in 2023 Version control added COMPLETE Name of standard changed to 'LOCS:23 Standard v10.2' and references amended throughout. NB. consider how this will work going forward for any future revisions.
			Either here or in the introduction it is possible to include ICO approval statement in line with other scheme criteria we have approved.	236. Include a statement of ICO approval in the document as follows: 'The certification criteria contained within this document have been approved by the Information Commissioner's Office in accordance with the	Statement added COMPLETE

				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.' However, this should be lined through until such time as it is approved.	
Contents page	Yes	p.2	Numbering is out of sync and page numbers are incorrect.	237. Once all recommended actions have been implemented, amend contents page so numbers are correct.	Amended COMPLETE
1.0 Introduction	Yes	p.3, para 1	This paragraph refers to law firms and barristers processing special category data, but there is no mention of criminal offence data which seems to be an oversight given that the scheme is for legal service providers.	238. Include reference to criminal offence data here. (See other comments about this under lawfulness.)	Added 'criminal offence data' after 'Special Category Data' COMPLETE
		p.3, 2nd bullet – Client Benefits	Not sure why 'Processed' has a capital 'P'. This is not a defined term (although 'processing' is.)	239. Uncapitalise 'Processed'.	Amended. COMPLETE
		p.4, para 2	Says, "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." But organisations are not meeting the certification – they are meeting the requirements to become certified.	240. Amend "to meet the LOCS certification" to say, '…needed to achieve certification against the LOCS standard', or 'to meet the LOCS certification requirements', or similar.	Amended to add 'requirements'. COMPLETE

7.0 Certification	Yes	p.12, para 2	Says, "An Organisation is able to certify as a Data Controller or a Data Processor." This wording is slightly misleading as the organisation wouldn't 'certify as' a controller/processor. Presumably this is intended to mean that both controllers and processors can apply for certification.	241. Amend wording to say, 'Both controllers and processors can apply for/obtain certification', or similar.	Amended as recommended. COMPLETE
Appendix 3 – Data Processor Control Applicability	Partially	Appendix 3	Once comments and actions above are taken into account this table may need updating.	242. Once actions are implemented update this table accordingly.	Table updated PARTIALLY Appendix 3 table has been updated, however the control reference LOCS:23:C9 says applies partially to processors. However, the alternative control box at **8.2.2** does not specify. See comment above re. action **no.97**. Amend the Processor Alternative Control and/or Appendix 3 as necessary.
P. Overall evaluation of criteria					
1. Do the criteria fully and adequately reflect all aspects of the scope (ie comprehensive criteria) to provide sufficient guarantees and meaningful, robust certification? [Annex 2 ref. 14a.]	Partially	n/a	All previous recommendations have been taken on board, but some minor amends are still necessary, including to the Annexes mapping the controls to the UK GDPR articles. The LOCS Standard is generally comprehensive, and, with a few exceptions noted in this document, the criteria provide for practical application of the UK GDPR to the processing in scope. Criteria are		

			mostly specific and measurable, although in some places wording needs refining. The LOCS Standard is overall easily understandable to the reader, including those with no knowledge of this sector. There is an issue with the wording regarding reliance on ISO 27001 to satisfy some of the security requirements which needs addressing. Once the required amendments detailed in this document are made the resulting certification should be robust enough to provide sufficient guarantees that the processing is carried out in a compliance with UK GDPR.		
2. Do criteria/supporting guidance include details of how compliance can be demonstrated for each criterion?	Yes	n/a	There is guidance to assist organisations in applying the criteria.	-	-
3. With respect to the scope (general or specific), are all relevant components of the processing operations (data, systems, and processes) addressed by the criteria? [Annex 2 ref. 4.]	Yes	n/a	All relevant components of the processing operations appear to be addressed by the criteria. It is now clear that the processing of criminal offence data is in scope.	-	-
4. Are the criteria commensurate with the size of the processing	Partially	n/a	There are some further amendments required regarding the public interest conditions and use of the Appropriate		

operation being addressed by the scope, the sensitivity of information and the risk of processing? [Annex 2 ref. 14b.]			Policy Document for processing special category and criminal offence data to ensure processing is lawful. Although the required actions have been largely addressed, there are some minor amendments required to ensure the principles are covered sufficiently.		
5. Are the criteria likely to improve data protection compliance of controllers and processors? [Annex 2 ref. 14c.]	Partially	n/a	Some minor amends still required to ensure the improved compliance of controllers and processors in scope, in particular relating to the principles and lawfulness. Mostly to clarify wording thereby ensuring the requirements are clear and accurately reflect the legislation, as well as some amendments relating to numbering/references.		
6. Will data subjects benefit in respect of their information rights, including explaining desired outcomes to data subjects? [Annex 2 ref. 14d.]	Partially	n/a	For the most part the scope and the criteria are written in clear language to help people understand how certification against this scheme will provide them with assurance that their data will be handled compliantly. All rights are covered, and now reflect that these apply to all data subjects, not just clients. Although some relatively minor amends are required.		