LOCS:23
Scheme Manual

Version 2.3
Released: December 2024

Welcome to LOCS:23 Certification.

The Legal Services Operational Privacy Certification Scheme (LOCS:23) is an official GDPR certification scheme as approved by the UK Information Commissioner's Office. Legal Services Operational Privacy Certification Scheme (LOCS:23) | ICO

For a certification to be viewed as a UK GDPR Certification Scheme Articles 42 and 43 of the UK GDPR need to be satisfied. Article 42 is the evaluation of a certification (standard) by the Information Commissioner's Office to verify that the content of the submitted standard would meet their expectation if assessing a business process against UK GDPR. Article 43 is the evaluation of a certification body (CB) that performs the conformance assessment against the published standard. This is undertaken by the UK Accreditation Service and follows a series of stages which includes a scheme review, CB assessment and then shadowed audits before finally, accreditation is issued.

ADISA is an existing UKAS accredited certification body and already runs a UK GDPR Certification Scheme and so is well versed in understanding the process of becoming a UK GDPR Certification Scheme. In order to add LOCS:23 to our accreditation roster we had to first undertake pilot audits of the standard itself to verify that the Standard is auditable. This was completed early in 2024 and the Standard is now under review by UKAS. A part of this review is that UKAS will require evidence of audits being carried out at each stage of the written audit process, so applications are now being accepted for certification to LOCS:23.

We are excited to be the certification body for this new Standard for the legal sector which can verify through independent third-party validation, compliance to criteria which are deemed as compliant with GDPR as determined by the ICO themselves.

We look forward to working with you to help you on your certification path.

Best wishes,
Steve Mellings.
Founder, ADISA Certification.
1st August 2024.

1.0 The Application Process

This document defines the process for becoming certified against Legal Services Operational Privacy Certification Scheme (LOCS:23 Standardv12.3) and for maintaining certification. Those companies seeking to be certified to LOCS:23 should read this document in conjunction with LOCS:23 Standard v12.3

This document is written in the second person with "you" meaning the representative of the applicant for certification and "applicant" means the company applying for certification.

Whilst the LOCS:23 Standard can be applied to a Data Controller and a Data Processor there is significant overlap between the two types of application and so a single Scheme Manual is presented.

If you are unsure whether your application is for Data Controller or Data Processor, you should contact ADISA via locs23@adisa.global where a further scoping conversation can take place.

1.1 Getting Started – Importance of the Internal Audit

There is a requirement within LOCS:23 8.5.1 to have an Internal Audit Process. If you have not carried out an Internal Audit at this stage, we recommend that you do so before progressing further as a copy of this Internal Audit will be required at Stage 1 of your application. A suggested template to use is included in your certification pack.

1.2 Certification Documents

Before progressing with your application, a Certification Agreement and Non-Disclosure Agreement will be issued electronically for your review and signature.

1.2.1 Non-Disclosure Agreement

As you will be the disclosing party, ADISA is happy to sign your own NDA to ensure your confidentiality is always protected.

1.2.2 Certification Agreement

This document serves two primary purposes; first to form an agreement between ADISA and yourself regarding the activities associated with becoming and maintaining certification. Secondly, it serves as the data processing agreement as you will be sharing a small amount of personal data with ADISA during the audit process. This document must be signed before any personal data is shared as part of the auditing process.

1.2.3 Licence Mark Agreement

At the end of the certification process, you will be required to agree to the Licence Mark Agreement which permits the use of the trademarked certification logo. This will be issued to you by the Certification Director as part of the award process.

1.3 Complaints

It is a requirement of ISO 17065 for the certification body to have a clear complaints process for complaints about the certification body's own activity and complaints about those companies who are certified by the certification body.

The ADISA complaints process can be found on our website here: https://adisa.global/complaints/

1.4 Communication with the UK Information Commissioner's Office (ICO)

For all UK GDPR Certification Schemes certified by ADISA, ADISA is required to communicate with the

ICO on all applications, award of certification and withdrawal of certification. You agree to this in 5.9 of the Certification Agreement and this is a mandated requirement of being certified by an approved GDPR Certification Scheme.

The ICO performs checks on applicants to ensure they are not under any investigation by themselves at that time. Should the ICO refuse an initial application then dialogue between all parties will be undertaken to resolve the situation. If the ICO does not permit the application to proceed then all application fees will be returned in full.

(NB: The ICO have requested ADISA to NOT inform them of applications ahead of the formal UKAS approval so until that point the ICO will NOT be informed).

1.5 Asking Questions

ADISA as a certification body is unable to consult but does appreciate that from time to time you may need further clarification on a criterion or a scenario.

For questions about your certification, and you are within an active audit, you should in all instances address questions to your auditor. This could be done during one of the frequent calls which take place during the audit process, or you can contact your auditor as you require. If the questions are simple in nature a response could be given verbally or in an informal email. If questions are more complex, your auditor will provide the answer to you in writing to create a record for both parties.

For questions you have when you are not in an audit OR where the question might impact others, you will be directed to the form on our website. Once received, your question will be answered within 3 working days, but if you have not received an answer in this time frame, please email questions@adisa.global.

For all questions which could impact others, for example clarification of a particular criterion within the Standard, the question and answer will be added to the guidance notes within each Scheme Manual.

1.6 Rejecting an application

As per Clause 4.4 – Non-Discriminatory conditions – of ISO17065 a certification body is permitted to decline an application for a variety of reasons including the following:

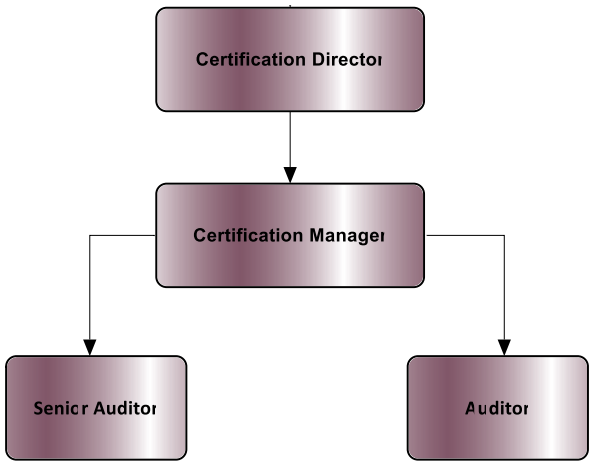
- Fundamental or demonstrated reasons why an application cannot be processed. (We do not believe you would be able to achieve certification)
- Applicant participating in illegal activities.
(We would need to have public domain evidence of this)
- History of repeat Non-Conformances with certification requirements. (Prior history with ADISA)
- Client related issues.
(Prior relationship issues with ADISA)

If an application is to be refused ADISA will contact the applicant directly clearly explaining the reasons why the application is being refused . An applicant can appeal directly to UKAS by contacting them by emailing customerfeedback@ukas.com and include full details. UKAS endeavour to reply within 5 working days.

2.0 The Certification Team

Once your application has been processed, you will be passed onto the ADISA certification team who will be responsible for working with all applicants to assess their compliance to LOCS:23 as part of the initial certification and then via the surveillance audit program to ensure ongoing compliance.

The structure of the certification team is as follows:



The Certification Director is responsible for ensuring each audit is carried out following the processes accredited by UKAS under ADISA's existing ISO 17065 certification.

The Certification Director is also responsible for ensuring that the business operates impartially and without bias throughout the certification process and will be the point of escalation throughout certification.

The Certification Manager is also a senior auditor and assumes the responsibilities of the Certification Director during absences. In all other ways, the Senior auditor and auditor have the same responsibilities which is to follow the ADISA audit process for each type of audit carried out.

You should always direct all audit questions to your allocated auditor and any question not directly associated with an audit to the Certification Director.

2.1 Auditor Allocation and your ability to object

When a new application is received and ahead of every LOCS:23 audit carried out, an impartiality assessment is made by ADISA regarding its auditors and all those who pass that process are presented to you as being approved to audit against LOCS:23 throughout the time you are certified with ADISA.

Should you feel that any of the named auditors may not treat you fairly, you can object to any of the auditors stating your reasons. How to do this is explained in the email you will receive listing the auditors who have been approved.

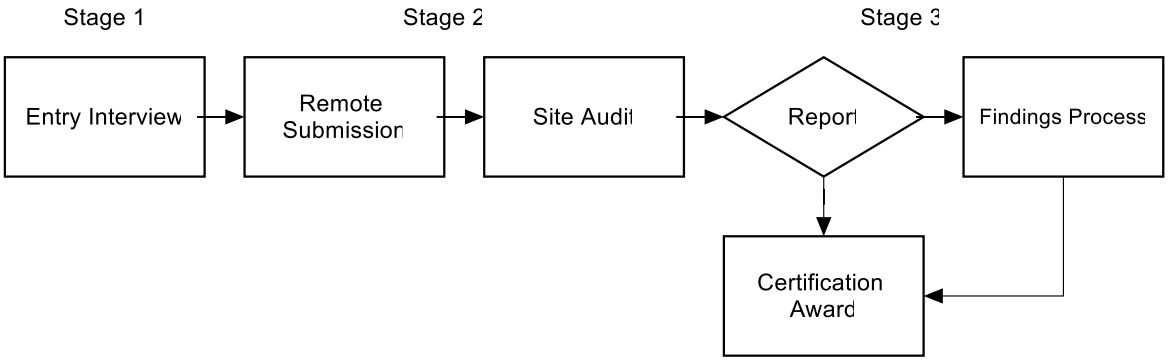
If you have no objections, an auditor will be allocated to you, and they will be your point of contact throughout the audit process.

If we do not hear back from you within 2 working days, we will presume that you have no objections to the auditors and will move forward with the process.

3.0 Audit Process

Once the Certification Agreement and NDA have been put in place (See 1.2) your application will be handed to your auditor. From this point, there are three stages to achieve certification each of equal importance.

Stage 1: Application Review.
Stage 2: Audit.
Stage 3: Audit Closure.



3.1 Stage 1: Application Review

The purpose of application review is to ensure the scope of the application is understood and that the applicant is well prepared and confident in their abilities to meet the requirements.

A copy of the internal audit document will be requested, and the auditor will review the completeness of this document ensuring that the scope of the application is understood. Where necessary they will ask for confirmation of certain details which will enable them to understand which internal, or external people may be required to participate in the audit.

Your auditor will then invite you to take part in an entry interview call and will suggest people who may be needed to participate. This call does not form part of the audit but is an essential part of Stage 1.

3.1.1 Entry Interview

The auditor will arrange a time to perform a remote entry interview to understand a range of aspects of the application. This call allows all parties to meet and discuss all aspects of certification around the following core agenda.

- Agree on the Scope of the application.
- Review and understand the person(s) or participants who are required for the certification process.
- Review of the internal audit as follows:
    - Discussion around any areas where the auditor feels that the audit might need more detail OR where the audit has highlighted an existing non-conformance.
    - Discussion of the certification process to be carried out in Stage 2 and what evidence might be required.

- Determine whether the auditor feels the applicant is ready to proceed to Stage 2 and if not, what is required to be done to proceed.

This call is expected to take between 1 and 2 hours during which the auditor will have open dialogue with the applicant resulting in one of the following next steps:

- Proceed to Stage 2
  Auditor has reasonable assurance based on the internal audit that the applicant is ready to proceed to formal evaluation.
- Undertake some remediation before proceeding to Stage 2
  Auditor believes that after agreed remediation that is to take place before Stage 2, that the applicant will then be ready to proceed to formal evaluation.
- Unable to proceed to Stage 2
  At this time the applicant needs to undertake remediation in order to be able to proceed. (See 3.1.2)

After the entry interview, the auditor will present a simple bullet point email back to the applicant outlining the discussion and highlighting any areas where remediation has been agreed upon and if they are unable to proceed, the reasons for this will be clearly outlined.

3.1.2 Unable to proceed

During the entry interview call the auditor will have open dialogue on areas where they feel the applicant would not be compliant and suitable remediation could be agreed on that call. Should that remediation require a significant amount of time to be carried out, or the applicant cannot commit to the remediation, then the application will be classed as unable to proceed and put on hold.

When an application is put on hold the auditor is removed from the application and it is returned to the Certification Director. They will liaise with the applicant to ensure they fully understand what is required and what the next steps should be.

When an applicant whose application is on hold believes they are now ready to progress, Stage 1 will be repeated. There is no charge to repeat Stage 1, but should the applicant be unable to proceed for a second time the certification director will set up a call with the applicant to fully understand the issues and a plan will be agreed on whether to proceed to Stage 2 regardless, or to reject the application in full.

3.2 Stage 2: Audit

To achieve certification, the applicant must pass Stage 1 to proceed to the formal audit process. This process is carried out in two parts: remote assessment and site assessment.

3.2.1 Remote Assessment

LOCS:23 has requirements to assess many policy documents and the remote assessment has the objective of allowing the applicant to submit documents for review by the auditor.

This stage allows the auditors to review complex documents without needing to be on your premises and to document conclusions without time pressure. Typically, the documents to be required are as follows:

- Record of Processing Activities TEMPLATE.
- Personal Data Breach Policy.
- Data Subject Rights Policy. (Data Controller only)
- A list of all Third-party suppliers that process the Client File.
- A URL or copy of your Privacy Notice.
- Data Protection Training Records.
- Business Continuity Plan .
- A Systems Document/Map.
- Security Policies.

Once the submission is received, the auditor will annotate the audit document with their analysis but will not report back on any findings. Where aspects of this submission require discussion, they will add that to their site audit plan.

3.2.2 Site Audit

On the agreed audit day, the ADISA auditor attends your site and conducts the practical part of the audit where they assess the implementation of policies shared. This audit will be conducted via face-to-face interview and will typically request access to the same personnel with knowledge of the following:

- Person designated with LOCS:23 compliance.
- Person designated with Data Protection compliance.
- Personnel familiar with the creation and maintenance of the Client File.
- Personnel familiar with IT Systems.
- Personnel familiar with Data Ecosystems such as routinely used data processors/data controllers.

The site audit is used to finalise understanding of key processes and to seek evidence of processes being operationally active.

The output from this stage will be the final completed audit document, although the auditor does reserve the right to ask for clarifications / additional information as required.

3.3 Stage 3: Audit Closure

Following the site audit the auditor will consolidate all parts of the audit into the audit document, which then goes through a period of internal review to ensure the document is complete and consistent. At that point, the auditor will provide an initial audit document including an audit report

and, if appropriate, the findings report and will arrange an audit wash-up call.

3.4.1 Audit Wash - Up Call

The purpose of the audit wash-up call is as follows:

- To allow you to query any aspect of the document presented.
- To discuss the next actions whether that might be a “Pass” award being made or going through the findings which have been identified.

The call CANNOT be used to present additional evidence, nor to offer mitigations for the audit findings as these need to be addressed within the findings process which is outlined in 6.0.

If you disagree with the report and the auditor maintains their position, you can appeal against the findings by following the appeal process which is outlined in 6.4.

If you agree that the audit document is a true reflection of what was seen on audit day, the audit document result is confirmed, and the process outlined in 3.5 followed.

3.5 Award or Findings Report

Once the audit document is closed, the following actions are taken:

- When the award is a recommendation for certification, the award process is followed as per 4.0.
- When there are findings from the audit, the findings process is followed as per 6.0.

4.0 Award Process

At the conclusion of and/or the findings process (6.0) your auditor will email you and inform you of their recommendation. The audit is then passed to the decision maker, the Certification Director, who will conduct the final checks before making the award.

During this process, the ICO will be informed of the intention to make the award and will carry out their own compliance checks before any award can be made. This typically takes 5 working days.

The Licence Agreement (See 1.2.3) will be required to be signed before the award can be made. The Certification Director will send the award email including the following:

- Copy of the audit document.
- Copy of the findings report. (If appropriate)
- Copy of the certification report.
- A letter confirming the award.
- Link to the certification page on our website.
- Certification certificate. (If first audit or if any changes to the previous version)
- Certification logo. (If first audit or if any changes to the previous version)

At this point, ADISA will make a social media announcement which is the same format for every successful company, and you will now be certified to LOCS:23 reverting to the audit schedule as per the normal audit process. (See 3.0)

5.0 Maintaining Certification

Following a successful full audit, you will be viewed as being ADISA Certified to LOCS:23 moving to a Surveillance audit cycle. Surveillance audits are carried out annually and will be approximately 40% of the entire Standard and will feature criteria from each section of the Standard.

A surveillance audit plan will be issued to you 30 days prior to the audit date, and this will also include any areas from previous audits which are required to be assessed again. These typically will be where corrective actions were agreed upon or where observations were made about a process potentially being non-compliance with a change in the operational environment.

Any issues at a surveillance audit follows the findings process (6.0)

Every three years a full audit is undertaken.

6.0 Findings Process

During an audit, the auditor may identify where the applicant under evaluation is not meeting specific criterion or there might be areas for concern on the applicant's ability to maintain compliance. In all such cases, the auditor will denote their conclusions on their audit document using the following status:

Status	Description	Corrective Action
Observations	Applicant has provided sufficient evidence or reasonable assurance to demonstrate a compliant position, but auditor recommends further review of this criterion to ensure ongoing compliance is achieved. (Example: A policy is missing certain requirements of the Standard but during discussion, the applicant was able to confirm that the criterion requirements are being achieved or measures are being put in place to achieve a compliant position within an acceptable time frame). An observation may also be made where a change in circumstances may impact an applicant's ability to maintain compliance with the Standard. (Example: A detailed policy does not exist to facilitate the use of sub-processors, as none are used. Should this business deliverable change, a policy should be created to control this	Observations are listed within the audit document and require no corrective action or response from the applicant but will be assessed at the next audit and will be added to Matters Arising.
Finding	A finding will be where the auditor has limited assurance of compliance with the mandated requirement of the Standard.	Findings are listed within the audit document and findings report. They must be addressed with a corrective action plan submitted by the applicant and accepted, with evidence, by the auditor.
Not Mandated	Within LOCS:23 Standard there are criteria which are not mandated to be met to achieve certification. During the audit these will be assessed by the auditor, but for the purposes of certification award,	None

	they will all be denoted as "Not Mandated."	
Not Applicable	This is where a mandated criterion within the standard has been identified as being not applicable to the applicant under evaluation. For the purposes of the certification award, they will be denoted as "Not Applicable."	None

Where there are findings, the audit cannot be recommended for an award of certification and the findings process is followed.

It is worth noting that it is absolutely normal to have findings identified during an audit.

6.1 Findings Report

Where the auditor has identified findings, they will create a findings report which will be a cut-down version of the audit document displaying only those criteria which require attention.

This report is then sent to you, and you are required to complete the document with your suggested corrective actions in order to close out the finding. The corrective actions for findings typically fall into three categories:

- Submission of additional evidence to verify current position as being compliant.
- Evidence of a corrective action which has already been done to move you to a current compliant position after audit day.
- A description of an intended corrective action along with a timeline of events you would undertake in order to move you to a complaint position at a point in the near future.

Your response should evidence this and will be evaluated using the SMART metric.

- **S**pecific – Does the correction action address the non-conformance?
- **M**easurable – Would ADISA be able to measure the corrective action to ensure it has been implemented?
- **A**chievable – Does the applicant have the capability to deliver on the corrective action?
- **R**ealistic – Is the timeline suggested realistic to achieve the corrective action?
- **T**ime Bound – Is the timeline suggested acceptable to ADISA?

6.2 Closure of Findings Report

When evaluating the corrective action plan suggested by you, the auditor will assign a response to each criterion as meeting one of the responses shown in the table below.

Non-Conformance Status	Description

Not agreed	The applicant's suggested correction would still not take the applicant to a compliant position. The timeline suggested by the applicant to carry out the correction is too long to be accepted by the auditor. The applicant is refusing to take corrective action or decided to not take corrective action.
Accepted Evidence Received	The applicant has been able to provide additional evidence either that they were compliant at audit OR that corrective actions have been undertaken and are in place.
Accepted Time-Bound	The applicant has presented evidence which would move them to a compliant position, but the action has not been undertaken. The timeline and intent are accepted by the auditor and the action is added to matters arising to be checked at the next audit.

Where a corrective action may not be accepted, a second opportunity will be given to put an acceptable action in place. Throughout this process, your auditor will be available to help you understand what the non-conformance is and reasons why the suggested corrective action may have been rejected.

It is our experience that this communication leads to resolution in all cases other than where a decision is made to cease certification efforts.

When agreement has been reached on the actions within the findings the audit moves to award (See 4.0).

Should an agreement not be reached you will receive an email from the Certification Director which includes the following:

- Copy of the audit document.
- Copy of the findings report.
- A letter confirming the audit result (Failure) and outlining the next actions.

At this point a conversation will take place about whether the applicant wishes to purse certification and if so, what action plan should be followed. Any attempt at recertification would require a full re-audit.

6.3 Understanding Timebound Corrective Actions

A time-bound corrective action would be where you suggest how a finding could be rectified and can put in place a plan to take the necessary action. If the auditor agrees and accepts a time-bound corrective action, these are listed within the applicant's matters arising file and will be checked at the next surveillance audit. If at the next surveillance audit, these corrective actions have not been carried out the auditor will assess, taking into consideration the type of finding, and decide whether the failure to take the corrective action previously agreed could result in a current audit failure OR whether they are prepared to let you rectify the previously agreed finding.

Throughout this, the auditor will communicate with you to ensure you are aware of the issues in good time.

6.4 Appeals Procedure

The appeals procedure is open for use at any time when you might feel that the behaviour of ADISA is biased, lacking impartiality or unfair. To make an appeal you should request a copy of the Audit Appeal Form from the Certification Director - lisa.mellings@adisa.global.

Examples of acceptable grounds for appeals at this point might be:

- The auditor was not impartial throughout.
- The auditor did not display knowledge of the industry/standard.
- The business suffered an exceptional issue during audit day and so we were not operating as business as usual.

Examples of not acceptable appeals might be:

- We knew about that and were going to fix it.
- We've told EMPLOYEE NAME that lots of times.

Should you feel that your reasonable concerns are not being fairly assessed, you can escalate your appeal. See 6.4.1.

6.4.1 Appeal Escalation

In situations where you feel that your appeal has not been handled fairly then there is a final level of escalation which can be made directly to the CEO, Steve Mellings. This should be via email to steve.mellings@adisa.global and include details of the grounds for escalation. This must be received within one working day of the initial appeal being rejected. A call will be set up within one working day of receipt of your email with the outcome being the final ADISA position on the matter. This will be documented and returned to you on the same day as the call.

Appendix A: Guidance Notes (See 1.5)

8.1.4 Data Protection Principles	
Criterion 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 to ensure records are not misleading.
Guidance or Clarification	
When an 'opinion' wherever from (lawyer, barrister, witness, other third-party), is documented as part of the case file it should be clearly indicated as such including whose opinion it is so that if incorrect (not accurate) it can be handled in a way that will not cause detriment to the data subject."	

8.3.9 Data Protection Training	
Criterion 8.3.9.2	The Data Protection Training where electronic SHALL include a knowledge test with a minimum of 80% pass mark.
Guidance or Clarification	
8.3.9.2 only applies in instances where electronic training is given and there is no requirement for a knowledge test specified within the standard for other training.	

8.3.9 Data Protection Training	
Criterion 8.3.9.6	The Data Protection training SHALL be delivered at regular intervals (at least annually).
Guidance or Clarification	
8.3.9.6 does not specify electronic training and so all applicants shall provide at least annual data protection training which could be electronic or by some other means. Please see guidance NB1 within section 8.3.9 in LOCS:23 Standard v12.3for recommendations for what could be included in such training.	

8.3.1 Data Protection by Design and Default	
Criterion 8.3.1.9.9	An Organisation SHALL use one or more privacy-enhancing technologies (PETs) to assist it in complying with its data protection by design obligations.
Guidance or Clarification	
In order to understand how to comply with this criterion the applicant should review the ICO guidance on PETs which can be found here. Written evidence of an assessment of the applicability of PETs would be required to be submitted where no PETS are being implemented. **Privacy Enhancing Tools:** Scheme Owner uses a definition of PET as provide by the EU Network for InfoSec (INESA) - 'software and hardware solutions, i.e., systems encompassing technical processes, methods or	

knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.'

In simple terms this could include:

- Pseudonymisation
- Two factor authentication
- Network segregation
- System segregation
- Access control

8.2.3 Right of Access	
Criterion 8.3.3.8	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.

Guidance or Clarification

Self Service Mechanism

Where Document Management Systems are used many have functionality for data subjects to be allowed to update their data directly. Where this functionality is not available or DMS are not used, a self-service mechanism could be the use of an online form or other mechanism whereby the data subject can make a request on the business independently from the business. To be defined as "self-service" the process must acknowledge the request and confirm that action is done without further prompting from the data subject.

8.3.7 Technical Security Measures	
Criterion 8.3.7.1	An Organisation SHALL document the core business systems processing in a systems map, clearly identifying those that process Client File data.

Guidance or Clarification

Systems Documentation.

Any system which is used to process the Client file should be documented in such a way that the Hardware and Software can be identified. This 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

8.3.7 Technical Security Measures	
Criterion 8.3.7.9	An Organisation SHALL have a policy in place governing the use of encryption, including approach to encryption at rest and in transit. The policy SHALL include the requirement for staff training as to the appropriate use of encryption for Client File Data at rest and in transit.
Guidance or Clarification	
Encryption The use of encryption for data at rest and in transit is a mandated technical security measure. The use of NIST Advanced Encryption Standards (AES) is required and applicants should review here: Advanced Encryption Standard (AES) | NIST	

8.2.1 Transparency & Communication	
Criterion	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.
Guidance or Clarification	
Applicant shall adopt plain language in all communications which can be defined as: Concise. Transparent. Intelligible. Easily accessible.	

Appendix B Document Changes – Scheme manual

Change from v2.0 – v2.1 25.11.2024

CIA / N/A	Where is the change	Change made	Version Number
CIA 130	Multiple Places	Update the document with the new version of LOCS:23 V12.2 – v12.3	V2.0 – v2.1

Change from v2.1 –v2.2 27.11.2024

CIA / N/A	Where is the change	Change made	Version Number
CIA 132	Page 13 - 14	Changes to the verification of what the auditor has provided to the auditor and adding observations will be added to matters arising	V2.1 – v2.2

Change from v2.2 – v2.3 04.12.2024

CIA / N/A	Where is the change	Change made	Version Number
CIA 134	Section 1.0	Addition of the process should ADISA reject an application.	V2.2 – v2.3