oyster ims*

Data Protection White Paper

Using your legal document management system to become UK GDPR certified

Many companies tell their clients that they are UK GDPR compliant, but can they prove it?

LOCS:23 is the only ICO approved data protection certification for legal services providers to prove compliance with the UK GDPR. The LOCS:23 standard comprises of 34 controls, many of which are either IT related or IT assisted.

Being a data protection certification naturally means that data is at the centre of the LOCS:23 standard and **the effective management of your client files is key to proving compliance**.

Background

On 1st February 2024, the ICO approved the LOCS:23 standard under Article 42 of the UK GDPR as the data protection certification for legal services providers to prove compliance with the UK GDPR, in line with the accountability principle.
LOCS is an acronym for: Legal Services Operational Privacy Certification Scheme.

Gaining an ICO approved certification helps demonstrate to clients, other businesses, and other regulators that your organisation can be trusted to process and protect their personal data in full compliance with the requirements of the UK GDPR, including data protection by design and by default, appropriate technical and organisational measures ensuring data security, and as an appropriate safeguard for data transfers to third countries. In addition, should a data breach unfortunately occur, the latest ICO Fining Guidance mentions certification as a mitigating factor under Article 83.2(j).

Finally, certification should make it easier for legal services providers to comply with outside counsel guidelines. Reviewing the controls in the LOCS:23 standard, it is clear that the effective management of your client files is key to proving compliance. Ensuring effective client file management from creation to destruction or archival requires the use of a document management system.

What features should your document management system have?

- ✓ Manage your files in line with your retention and destruction Policy (‘storage limitation’ principle).
- ✓ Secure your files from unauthorised access, accidental loss, destruction or damage (‘integrity and confidentiality’ principle).
- ✓ Allow you to find and export all relevant data relating to a Data Subject Access Request quickly and easily.
- ✓ Allow you to use secure methods of transferring data from your document management system.
- ✓ Have the security benefits of a cloud hosted ‘Software-as-a-service’ (SaaS) platform to ensure management of security patches and control of client file backup and restore processes.

Breaking this down further, your document management system should:

Allow you to easily create and apply retention policies either at the whole client file level or specific to record types within the file	→	iManage Work + iManage Records Manager
Have access management features that allow you to simply control who has access to files and ensure that only those employees that need access receive it	→	iManage Security Policy Manager
Implement NIST Advanced Encryption Standard (AES) encryption to files at rest for added protection	→	Encrypted database and document stores in iManage Work, iManage Records Manager, iManage Share
Have auditing controls to prove who has accessed files and when	→	iManage Work
Allow you to meet the deadlines of a Data Subject Access request (DSAR) with fast search and export capabilities, whilst ensuring that your access controls are respected.	→	iManage Work, iManage Share
Have instant secure link functionality to reduce the need for export and allow selected outside parties, including clients, access to files in a controlled manner	→	iManage Share
Apply security patches as soon as they are available	→	iManage Cloud
Make it easy to manage backups and be simple to restore those backups if required	→	iManage Cloud

What is certification?

UK GDPR provides for the creation of official certification schemes that will be recognised by the Information Commissioner's Office.

ICO certification requirements include:

- **UK GDPR** - The standard must meet all UK GDPR requirements.
- **SCOPE** - The standard must have a defined scope that relates to a specific processing activity.
- **PRACTICAL** - formulated in such a way that they are clear and allow practical application.
- **AUDITABLE** - objectives must be specified along with how they can be achieved, to demonstrate compliance.
- **RELEVANT** - to the target audience.
- **INTEROPERABLE** - with other standards such as ISO 27001.
- **SCALABLE** - for use by different sized organisations.

The UK certification body for LOCS:23 is ADISA.

The certification process

Submission
When you believe your organisation is ready, submit a formal application for either data controller or data processor certification.

↓

Certification Agreement and NDA
ADISA set up a Certification Agreement and an NDA to formalise the application, and inform the ICO for validation. After submission and fee payment, you will receive a Scheme Manual providing detailed guidance on the certification process, including standard criteria, evidence requirements, and compliance examples.

↓

Pre-Audit Assessment
An auditor reviews your application's scope and parameters. They discuss the internal audit with you and confirm your organisation's current status and compliance plans. The auditor confirms scope, key personnel and systems, and you jointly plan the audit schedule.

↓

Audit Process

- Remote Review: Auditors assess documents for standard conformance via a secure SharePoint site.
- On-Site Audit: At your main operational site, with a pre-shared schedule to ensure stakeholder availability.
- Reporting

↓

Certification
Auditors compile an audit report assessing each criterion. Full conformance is required for certification. Auditors may request extra evidence or clarifications. Successful audits result in certification, while non-conformances must be addressed before certification is granted.

Conclusion

LOCS:23 certification allows your organisation to prove it meets all the requirements of the UK GDPR and is a trusted data controller or data processor. A fully functional, cloud hosted document management system eases and supports your journey to certification.

Author

Oyster IMS is a LOCS:23 Registered Consultancy, qualified in implementing the LOCS:23 standard, and with proven expertise in data protection legislation.

We have several Approved Implementors, who provide consultancy support and implementation services to organisations wanting to comply with the LOCS:23 standard and prepare for officially recognised certification.

iManage
Implementation Partner

Oyster IMS is also an iManage implementation partner. Built on more than 20 years of experience, iManage helps leading organisations manage documents and emails more efficiently, protect vital information assets, and leverage knowledge to drive better business outcomes.

London

+44 (0)207 199 0620
info@oyster-ims.com

The Loom
14 Gower's Walk
London E1 8PY

Dublin

+353 1 584 6686
info@oyster-ims.com

Carrick House
49 Fitzwilliam Square
Dublin 2

✉ info@oyster-ims.com
🌐 www.oyster-ims.com
in oyster-ims
𝕏 @oysterims

oyster ims*