

**L**EGAL SERVICES  
**O**PERATIONAL PRIVACY  
**C**ERTIFICATION  
**S**CHEME



March  
2024

LOCS Practitioner Study Guide

# Introduction

---

The LOCS:23 programme is the first official ICO approved UK GDPR certification for legal services.

LOCS:23 is a principles-based data protection compliance standard encompassing UK data protection laws, key privacy terminology, and practical concepts concerning the protection of personal data and trans-border data flows in a legal services environment.

The LOCS:23 Practitioner accreditation is for those individuals intending to support their organisation in maintaining compliance with the LOCS standard. credential specific to European data protection professionals that is part of a comprehensive

The LOCS Practitioner course is designed to cover:

- Data Protection best practice
- Information Security best practice
- The fundamentals of the LOCS standard

## LOCS:23 Scope

---

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

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

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

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

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

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.

## 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

## Processing Activities in Scope

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

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

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



## **Types of Organisations in Scope**

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

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

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

### **Data Controllers within scope**

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

### **Data Processors/Sub-processors within scope**

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

## **The LOCS:23 Standard**

---

The LOCS:23 standard is the criteria by which a legal services organisation can measure its compliance with UK GDPR either as a Data Controller or Data Processor.

The LOCS:23 standard has 34 controls divided into 5 core areas:

### **1 ORGANISATIONAL AND CLIENT FILE GOVERNANCE**

### **2 CLIENT RIGHTS**

### **3 OPERATIONAL PRIVACY**

### **4 THIRD-PARTY SERVICE PROVIDERS AND DATA SHARING**

### **5 MONITOR AND REVIEW**

The standard uses the following format:

<b>CONTROL REFERENCE</b>	<b>This is used to identify each control section</b>
<b>CONTROL OBJECTIVE</b>	This is the outcome desired from the control's implementation.
<b>CONTROL</b>	This is the detail of the control applicable.
<b>CONTROL APPLICATION GUIDANCE</b>	This is practical guidance, notes and comments.
<b>DATA PROCESSOR ALTERNATIVE CONTROL</b>	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.
<b>UK GDPR REFERENCE</b>	This is the UK GDPR Article that the control relates to where applicable.
<b>AUDIT REFERENCE</b>	This is used to cross reference the Self-Audit Schedule. See template in Appendix 4.

## Who is the course aimed at?

The LOCS Practitioner course is aimed at anyone who intends to support LOCS compliance within an organisation. This may include key individuals from

- Compliance
- IT
- Data Protection team
- Other relevant support functions

## Benefits

### Benefits to the organisation

Organisations can benefit in many ways by complying with the LOCS:23 standard. These include:

- Promote Client confidence by demonstrating you are certified to protect their personal data.
- Have a competitive advantage.
- Officially recognised
- Apply a recognised, measurable and auditable data protection standard across the organisation.
- Save time and resources completing Client data protection questionnaires.
- May be used as a 'supplemental measure' for international transfers.
- Mitigate against ICO enforcement action (Art 83).
- Compliments the ISO 27001 standard for information security.
- Continuously updated with emerging ICO guidance and input from LOCS:23 fellows.

- Simplify procurement process with LOCS:23 certified vendors

### Benefits to the individual

- Demonstrate knowledge of data protection and information security fundamentals
- Internal career development
- Enhanced CV

## Preparation

---

In general, we recommend that you plan for around 2 hours of study time in advance of taking the knowledge test however, you might need more or fewer hours depending on your existing knowledge of the core areas and professional experience.

We recommend you prepare in the following manner:

### 1. Review the LOCS:23 standard

The standard is available to download free of charge from the ICO website [here](#)

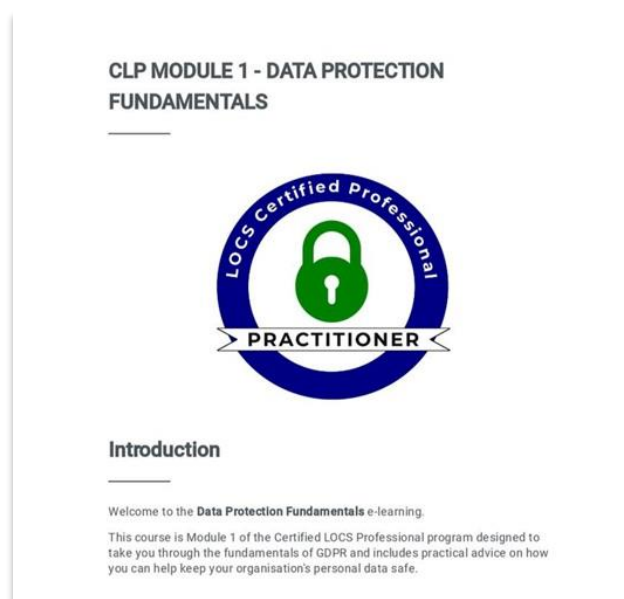
Review the standard to understand the core requirements and controls structure.

### 2. Revise Data Protection fundamentals

Although all key areas are covered in the LOCS Practitioner e-learning, a working knowledge of UK GDPR and the fundamental principles will be advantageous.

## MODULE 1 Course structure

---



## Introduction

### Data Protection Principles

- The 7 Principles

### What is Personal Data?

- Types of Personal Data

### Data Subject Rights

- Know Your Rights

### Data Protection Best Practice

- Data Protection Impact Assessments
- Dealing with a Request for Access to data
- Identifying & Reporting a Data Breach
- Engaging Third Parties
- Sharing Personal Data
- What Can I Do? (Dos)
- What Can I Do? (Don'ts)
- What to do when....

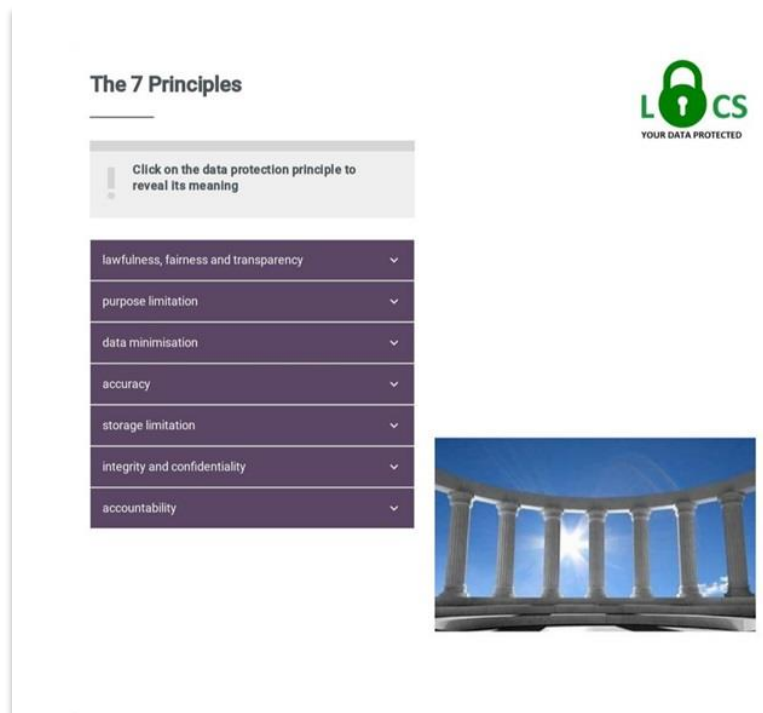
### Recent Penalties

- Action Taken by the ICO

### Quiz

## EXAMPLE CONTENT

### Principles



The 7 Principles

Click on the data protection principle to reveal its meaning

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountability

L1CS  
YOUR DATA PROTECTED

## Personal Data

### Types of Personal Data

UK GDPR defines 'personal data' as anything identifiable to a living person. Some personal data is regarded as 'special category data' - drag and drop to match the data type with the data category

Place the data type on the correct pile

Ethnicity

Personal Data

Special Category Data

## EXAMPLE QUIZ QUESTION

### Personal Data

Which of the following are NOT special category data (select all that apply)

- Payslip
- Doctors Note
- Bank Details
- Driving Licence
- Diversity Details



## MODULE 2 Course structure

---

**Introduction**

---



Welcome to the **Data Protection for Remote Workers** e-learning.

This course is Module 2 of the Certified LOCS Professional program designed to take you through the fundamentals of GDPR and includes practical advice on how you can help keep your organisation's personal data safe.

### **Introduction**

#### **Information Security Objectives**

- Protecting your data
- The consequences of insufficient security

#### **Passwords**

- Password Best Practice

#### **Safe Web Browsing**

- Look for the Padlock
- Look for Https
- Look for a certificate
- Popups - Malware
- Popups - Scareware

#### **Email Security**

- Email Do's & Dont's

#### **Device Security**

- Devices at home
- Physical Security
- Paper Documents

## Scams

- Email Scams
- Telephone Scams

## Quiz

## EXAMPLE CONTENT

### Passwords

Password Best Practice

Click on the password category to see the advice

- Password Admin
- Types of Passwords
- Password Best Practice

### Devices

Devices at home

Click on category to see advice

- Laptops
- Mobile Phones
- Memory Sticks
- Home Broadband

## EXAMPLE QUIZ QUESTION


DOs & DON'Ts

Using drag and drop match the headings with their correct descriptions

Sort the cards below into their corresponding categories.


Send work documents to your personal email account

DOs      DON'Ts




## MODULE 3 Course structure

---



CLP Module 3 - LOCS Fundamentals



Welcome to the LOC:23 **LOCS Fundamentals course and Certified LOCS Practitioner** assessment.

This course is designed to introduce you to the fundamentals of LOCS:23, how it applies to Legal Services and assess your knowledge of UK GDPR and the LOCS:23 standard.

Upon successful completion of the knowledge test (80% pass) you will

- be certified as a LOCS Practitioner
- receive a hard copy of the LOCS standard
- use the 'LOCS:23 'Certified LOCS Practitioner' logo

### Introduction to official Certification Schemes

## Certification Benefits

### Introduction to LOCS:23

### LOCS:23 Standard Scope

### LOCS:23 Ecosystem

### Key Roles

### Approved Implementor Benefits

### Certified LOCS Practitioner

### Key Roles 2

### LOCS:23 Standard overview

## EXAMPLE CONTENT



### Official Certification Schemes

#### Introduction

Art 42 of the GDPR and UK GDPR provides for the creation of official certification schemes that will be recognised by the local Supervisory Authority (in this case the Information Commissioner's Office)

#### ICO Requirements

The primary requirements are:

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

The LOCS:23 Practitioner knowledge test has 30 questions that are a combination of multi-choice and select the best answer questions.

Two example questions below.

### Q19 - Lawful Processing

Which of the following lawful basis are UNLIKELY to be used by Law Firms?  
(tick all that apply)

- Contract
- Legitimate Interest
- Public Task
- Legal Obligation
- Vital Interests
- Consent

✓ Submit

### Q20 - Data Breach Management

Drag the answer to the appropriate location

Laptop stolen containing client medical data

Reportable Data Breach      Non-reportable Data Breach