oneAdvanced

GUIDE

Security and compliance for law firms in 2025

The role of legal software and how to obtain LOCS:23 certification

Contents

Introduction

According to recent surveys, the legal profession considers security and compliance to be their biggest challenge in 2025. High-profile incidents and fines over the last several years has revealed the significant risks of weak data protection for law firms, both financial and reputational.

To address the growing demand for accountability in the space, the Information Commissioner's Office (ICO) introduced the LOCS:23 certification scheme (Legal Operational Privacy Certification Scheme) to highlight those legal service providers complying with UK GDPR and managing their data using best practice.

For law firms aiming for best practice as far as their cybersecurity and data protection is concerned, LOCS:23 certification is something that should be aspired to, as you'll find on the next several pages.

Security and compliance for law firms in 2025

In 2025, security and compliance are critical priorities for law firms operating in a digital world. Firms handle highly sensitive data, including confidential client information and business intelligence. Safeguarding this data against cyberattacks and ensuring compliance is more urgent than ever

The National Cyber Security Centre reports that 65% of UK law firms have fallen victim to cybercrime, a stark reminder that legal professionals are key targets for cybercriminals. In addition, the data revealed that 27% of law firms had experienced some form of security breach, further underlining the urgency of strengthening cybersecurity measures.

Legal compliance means adhering to frameworks like GDPR, which govern how firms manage and protect data. For firms to effectively manage these risks, they must adopt high standards of compliance, coupled with robust security strategies that include proactive measures such as threat detection, employee training, and incident response plans. Compliance is not only a matter of avoiding fines but also a fundamental element of protecting client confidentiality business integrity, and reputation.

As the volume of data grows, firms increasingly use digital tools, cloud storage, and AI-powered automation to streamline operations. However, the adoption of these technologies also opens new attack surfaces, potentially increasing vulnerability to cyberattacks.

Moreover, client expectations have changed. In the always-on, fast-paced digital world, clients expect quick responses and secure, accessible communication channels. To meet these demands, law firms are adopting digital communication tools like online portals, encrypted email systems, and secure messaging platforms. But while these tools improve efficiency, they also introduce new security risks that must be managed carefully. Firms must balance the need for seamless client experiences with the imperative to protect sensitive information.

The legal sector is also grappling with the impact of AI and automation, which promise to increase productivity but also raise ethical and transparency issues. With AI-powered systems potentially introducing vulnerabilities if not properly secured, law firms must ensure that security considerations are central to their technology adoption strategies.

Staying secure and compliant in 2025 requires law firms to adopt a proactive and evolving approach to both compliance and cybersecurity. Regular security audits, continuous employee training, and partnerships with cybersecurity experts are essential for safeguarding client data and meeting regulatory requirements. Firms must also implement clear incident response plans to mitigate the impact of potential breaches. Whether large or small, law firms cannot afford to be complacent about these issues—compliance and cybersecurity must be at the core of their operations.

The importance of security & compliance for firms and clients

The importance of these practices extends far beyond regulatory adherence; they are vital for maintaining trust with clients and protecting a firm's reputation. Due to the sensitive nature of legal work, any data breach can lead to severe financial and reputational damage.

Security and compliance are critical due to the immense value of data law firms hold. Client data, including personal, financial, and business-related information, is a prime target for cybercriminals. A data breach involving client information can lead to substantial financial penalties under GDPR and other regulatory frameworks, as well as the loss of trust from clients. Legal professionals have an ethical responsibility to ensure client confidentiality. A breach can lead to financial penalties and reputational damage, potentially deterring future clients.

Firms also store a wealth of business-sensitive information, such as employee data and internal strategies. Protecting this data is crucial for safeguarding the firm's operations and ensuring business continuity. A cyberattack could expose trade secrets or internal strategies that could be exploited by competitors. Employee data, which may include personal details such as addresses and financial information, must also be protected to avoid putting staff at risk.

Compliance is equally important for ensuring that law firms operate within the boundaries of the law and industry standards. Regulators like the Solicitors Regulation Authority (SRA) set stringent guidelines that legal professionals must follow to maintain their practicing certificates. Adhering to these regulations is non-negotiable, and non-compliance can lead to severe penalties, including suspension from practice.

Beyond the legal and financial implications, building a strong culture of compliance and cybersecurity is essential for long-term success. Clients entrust law firms with their most sensitive information, and they expect that their data will be handled with the utmost care. A proactive approach to data security, such as conducting regular vulnerability assessments and maintaining strong access controls, helps build client confidence. It signals that the firm takes its responsibilities seriously and prioritises the safety of its clients' information.

Moreover, as cyber threats become more sophisticated, firms must keep pace with the latest security practices and technologies. Partnering with trusted technology providers and using advanced solutions such as cloud-based storage with encryption, multi-factor authentication, and threat detection systems can offer additional layers of protection. These tools not only help prevent breaches but also demonstrate to clients that their data is being handled securely.

In addition, having well-defined incident response plans in place ensures that if a breach does occur, the firm can respond swiftly and minimise the damage. This includes notifying affected clients, addressing the breach, and preventing further exposure. Transparency in handling data breaches is key to maintaining trust, and having a clear action plan in place can make all the difference in how a firm is perceived post-incident.

In light of increasing cyber threats, law firms must prioritise not only the prevention of breaches but also the implementation of robust response mechanisms. As regulations like GDPR enforce strict data protection standards, failure to comply can result in severe financial and reputational repercussions. Firms must therefore treat data protection as a key element of their overall risk management strategy.

The ICO, as the UK's data protection authority, oversees the enforcement of GDPR. Law firms found in breach of GDPR may face steep penalties, as well as damage to their reputation. This makes data protection an essential aspect of risk management in the legal profession.

Several high-profile breaches have emphasised the urgency for robust data protection. For example, in March 2022, leading criminal law firm Tuckers was fined £98,000 following a ransomware attack that exposed negligent security practices. This incident reinforces the importance of stringent data security measures.

To meet these growing demands for accountability and security, LOCS:23 was developed specifically for the legal sector. LOCS:23 certification ensures that law firms can demonstrate robust data protection measures and compliance with GDPR.

What is LOCS:23 certification?

LOCS:23, the Legal Operational Privacy Certification Scheme, is a UK GDPR certification framework approved by the ICO. It is the first certification designed specifically for law firms, barristers' chambers, and other legal service providers. The certification offers a clear, easy-to-follow set of standards to ensure that legal professionals handle client data securely and in compliance with GDPR.

Achieving LOCS:23 accreditation requires law firms to implement strict data protection policies, appoint responsible officers, and apply technical and organisational measures to safeguard client data. Firms must document compliance actions, manage data breaches, and ensure transparency in processing, thereby meeting ICO requirements.

LOCS:23 is becoming essential in the legal sector, much like Cyber Essentials in other industries. Public bodies, financial institutions, and corporate clients are likely to make LOCS:23 certification a precondition for engaging legal services, as it demonstrates the firm's ability to manage data securely.

Additionally, LOCS:23 certification is auditable, scalable, and designed to be interoperable with other security standards like ISO 27001. Law firms of all sizes can adopt the standard, making it applicable to sole practitioners, small chambers, and large international firms alike.

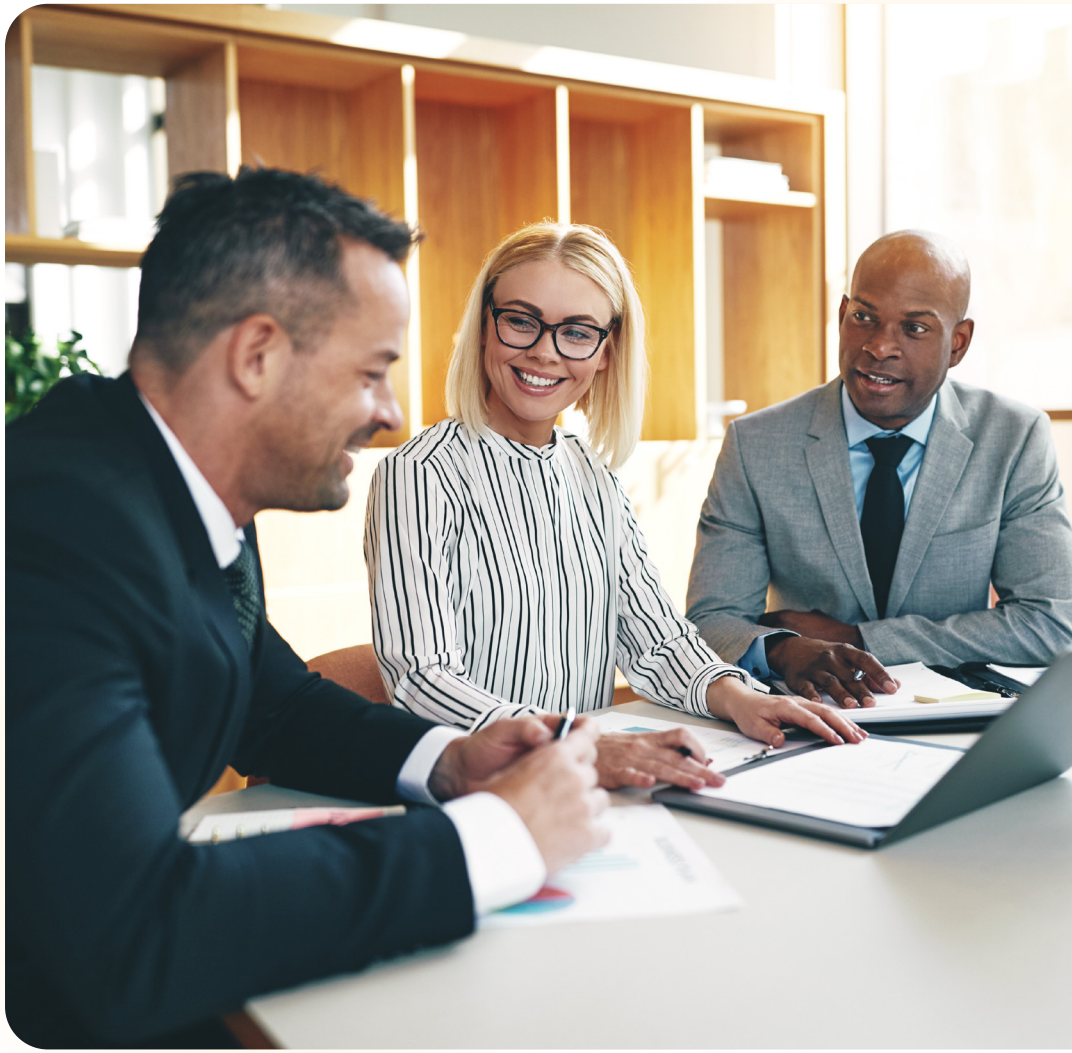
The core aspects of LOCS:23 include:

- **Data Processing Standards**
- **Security Measures**
- **Vendor and Supply Chain Management**
- **Data Subject Rights**
- **Breach Management**

Benefits of LOCS:23 certification

LOCS:23 certification provides several key benefits for law firms:

1. **Competitive advantage:** Firms that achieve LOCS:23 certification can differentiate themselves by demonstrating robust data protection measures, which is increasingly becoming a client expectation.
2. **Regulatory compliance:** The certification helps law firms align with UK GDPR, ensuring they meet their regulatory obligations and avoid potential fines.
3. **Risk mitigation:** By complying with the LOCS:23 standard, firms reduce the likelihood of data breaches and the financial and reputational damage that can result.
4. **Simplified procurement:** For law firms bidding for work with public bodies and large corporations, LOCS:23 certification can simplify procurement processes by offering a recognised standard of data protection compliance.



Implementing LOCS:23

One notable example of successful LOCS:23 implementation is the case of 30 Park Place, a Cardiff-based barristers' chambers. They became the first set of chambers to receive certification under the new ICO-approved GDPR standard. This achievement highlights the importance of data privacy in the legal sector and showcases how LOCS:23 can be leveraged to gain a competitive edge.

30 Park Place recognised the strategic advantage of adopting the LOCS:23 standard. As they say: "Achieving LOCS:23 is in our best interest, as it keeps us ahead of our competitors. We believe that law firms and local authorities will soon require this certification before instructing us, making it a crucial part of our business operations."

Strengthening data breach preparedness

One of the primary benefits of LOCS:23 certification is the enhanced preparation for data breaches. LOCS:23 equips organisations to manage their risks more effectively.

30 Park Place saw this aspect as one of the most significant advantages of pursuing LOCS:23. By adopting this standard they improved their internal data protection practices, incorporating additional security layers to mitigate the risk of breaches.

"By having LOCS:23, we are able to reduce the possibility and frequency of data breaches, as well as the associated costs. Additionally, our members are now required to complete annual training to meet their regulatory requirements."

This proactive stance helps organisations not only avoid potential breaches but also assures clients that their data is in safe hands.

The certification process

Achieving LOCS:23 isn't a single event but an ongoing process that evaluates data governance and security frameworks. For 30 Park Place, their certification journey was supported by Briefed, a leading consultancy in GDPR compliance and LOCS-approved training.

"Briefed were instrumental in completing a gap analysis of our data governance structure with an action plan that helped us get into the strongest possible position to be certified." This partnership ensured that the chambers were well-prepared for the final audit phase, and the continued support post-certification from briefed helped them maintain compliance long term.

Briefed is the only legal service supplier that has achieved the LOCS:23, giving them a true understanding of not only what it takes for a business to achieve and maintain this new standard but how effective the standard is. With this knowledge comes the only UK training modules recognised as meeting the requirements by the official LOCS:23 scheme.

By proactively addressing data privacy concerns, improving preparedness for data breaches, and working with experts like Briefed, legal firms can gain a significant competitive advantage in the market while protecting their clients' sensitive data.

How to apply for and obtain LOCS:23 certification

A structured approach is required to meet LOCS:23 certification standards. The certification process involves several stages, from initial assessment and documentation review to auditing and final certification.

Step 1: Internal assessment and planning

The first step in obtaining LOCS:23 certification is to assess your firm's current data protection practices. This involves a thorough review of existing policies, procedures, and security measures related to client data.

This internal assessment lays the foundation for the certification process and helps firms understand where improvements are needed.

Step 2: Documentation and policy review

Law firms must have comprehensive documentation in place to demonstrate their compliance with GDPR and LOCS:23 standards.

Training all relevant staff in GDPR compliance and their data protection roles is critical at this stage.

Step 3: Initial audit and gap analysis

Once the necessary documentation is in place, firms undergo an internal audit to assess their readiness for LOCS:23 certification.

Firms can work with external GDPR consultants, like Briefed, to conduct a thorough gap analysis and develop an action plan for addressing any areas of non-compliance.

Step 4: Remediation and implementation

After the audit, firms must implement the necessary changes to address any gaps identified during the gap analysis.

At this stage, ongoing monitoring and adjustments may be required to ensure that all areas of compliance are being addressed effectively.

Step 5: Certification audit

Once the firm is confident that it meets the LOCS:23 standards, it can apply for an official certification audit. An independent certification body, approved by the ICO, will conduct a thorough audit to assess the firm's data protection framework and confirm its compliance with the LOCS:23 standard.

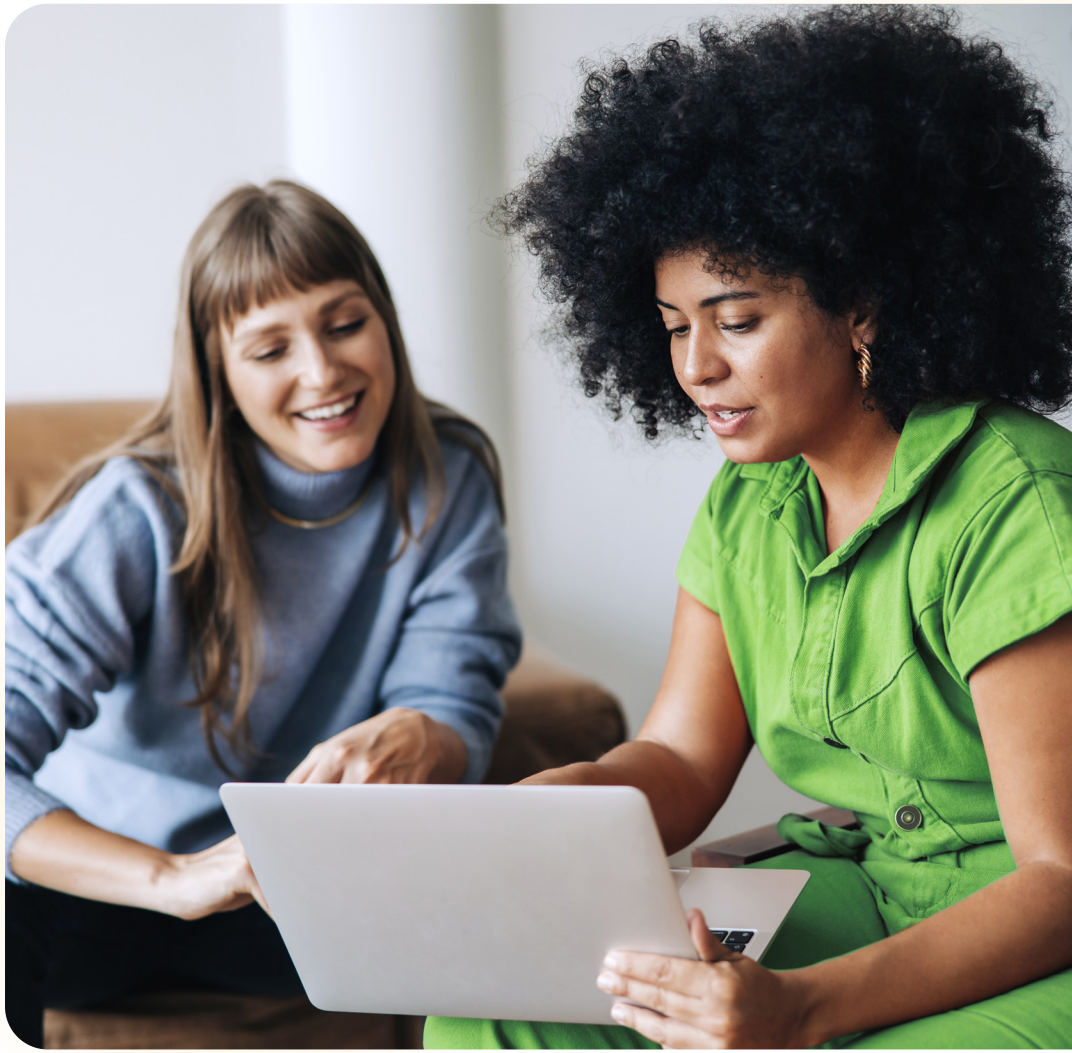
The audit process involves reviewing all documentation, policies, and practices to ensure they align with the certification's objectives.

If the firm passes the audit, it will be awarded LOCS:23 certification, which is valid for three years. Recertification will be required every three years, and annual audits and reviews are necessary to maintain compliance during the certification period.

How OneAdvanced helps

For law firms striving to achieve LOCS:23 accreditation, partnering with OneAdvanced, a trusted provider, offering legal professionals a secure, compliant, and streamlined path to accreditation through its suite of robust legal software solutions. As a reliable partner and data processor, OneAdvanced ensures that law firms can confidently meet the stringent data protection and operational standards set out by LOCS:23.

OneAdvanced's legal software is specifically designed to help firms manage their sensitive client data securely while ensuring full compliance with UK GDPR requirements. Through automated processes, integrated risk assessments, and strong data governance features, law firms can minimise human error, ensure secure data processing, and maintain an auditable trail of all data activities—key elements of the LOCS:23 framework.



OneAdvanced supports firms in their journey to LOCS:23 certification with:

- **Comprehensive data management:** OneAdvanced legal offers a unified platform to manage client data efficiently, including features for secure data storage, access controls, and data destruction policies. These capabilities align with LOCS:23's core requirements for safeguarding client information.
- **Compliance monitoring:** Solutions offer continuous compliance tracking, identifying areas that need attention and generating reports to ensure all GDPR requirements are consistently met. This reduces the administrative burden on law firms, allowing for real-time insights and proactive compliance adjustments.
- **Breach response and risk mitigation:** OneAdvanced's solutions are equipped with breach detection and response mechanisms, ensuring that firms can quickly identify and respond to data breaches. With built-in incident management tools, law firms can ensure they meet LOCS:23 requirements for breach notification and mitigate risks before they escalate.
- **Scalability and flexibility:** Whether a small practice or a large international firm, OneAdvanced's solutions scale to meet the specific needs of each firm. The software integrates with other compliance frameworks, ensuring interoperability with existing security protocols and further strengthening a firm's overall data protection strategy.

OneAdvanced Legal empowers law firms in achieving their LOCS:23 certification by providing a comprehensive security framework that prioritises data protection and compliance. With its secure cloud infrastructure, firms can confidently manage sensitive information, knowing it is safeguarded by robust data encryption. Additionally, regular security assessments and adherence to industry standards ensure that systems remain resilient against potential threats. This commitment to security not only supports accreditation efforts but also allows firms to build trust with clients by ensuring their data is in safe hands.

By leveraging OneAdvanced's legal software, law firms can streamline the LOCS:23 certification process and continuously maintain their accreditation through proactive security measures and compliance management.

As the legal sector faces increasing pressure to ensure robust data protection, LOCS:23 certification provides a structured framework for GDPR compliance. Law firms that achieve LOCS:23 certification can demonstrate their commitment to protecting client data, reducing the risk of breaches, and maintaining trust with their clients and regulators.

oneAdvanced

Powering the world of legal

OneAdvanced powers over 30,000 legal professionals with software automation that delivers increased productivity and agility, using modern security protocols and built-in regulatory compliance to help protect law firms from financial penalties and business disruption.

Our legal software suite includes practice and case management, time capture, document management, legal forms, The National Will Register, and performance & talent management.

Learn more

BRIEFED

Briefed are a team of experienced barristers who specialise in providing high quality training, certification and compliance support for businesses in the UK. For more information about how they can help you apply for the LOCS:23 accreditation, click here.

+44(0) 330 343 4000 www.oneadvanced.com hello@oneadvanced.com