oneAdvanced

OneAdvanced Legal
Security brief

OneAdvanced Legal is a modern cloud platform, developed to support firms in navigating the complexities of delivering vital legal services in a continually evolving landscape.

Developed with years of experience of the nuances of UK and Irish law, it replaces disjointed processes and siloed systems with a single platform that delivers secure flexible work efficiency, time savings, and faster matter turnaround.

OneAdvanced Legal safeguards your firm's security and protects it from threats, ensuring compliance with UK law and regulatory requirements, including GDPR, SRA, LAA, HMRC, and the Law Society. Built on Microsoft's Azure, our platform provides a secure and compliant infrastructure, leveraging the Azure landing zone to isolate and manage resources. This includes network security, identity and access management, policy-driven governance, consistent compliance, and secure DevOps integration, giving you peace of mind and allowing you to focus on delivering exceptional legal services.

This Cloud Security Document outlines the security measures and practices that OneAdvanced have implemented to protect both the platform. Further details can be found from the full OneAdvanced Legal Security Statement, [here](#).

Secure cloud infrastructure

- Cloud PCMS application is hosted on Microsoft Azure infrastructure.

- Single sign-on (SSO) allowing users to sign onto multiple independent software systems using one set of credentials.

- Multi-factor authentication (MFA) keeps users secure through electronic authentication method, only granting access after presenting two pieces of data.
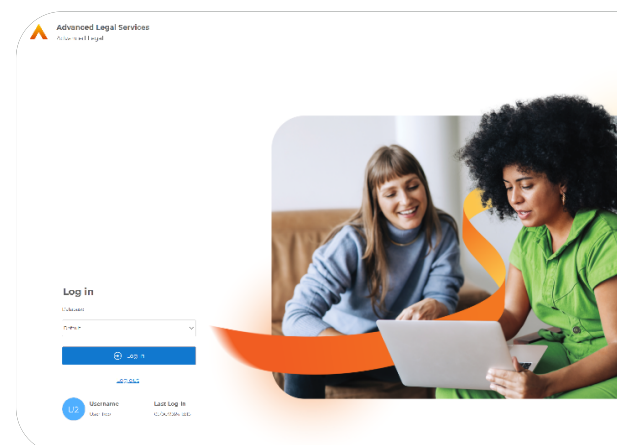
Data location and platform scalability

- OneAdvanced Legal PCMS data is stored in Microsoft Data Centres

- Microsoft Azure Auto-Heal automatically restarts parts of service which are not performing correctly

- National Will Register data resides in dedicated servers which are hosted in our Azure Data centre

- Legal Forms are hosed in Amazon AWS cloud environments and is protected by the standard AWS Security infrastructure and AWS Well-Architected Security Framework

Information security framework

- Regular risk assessments and risk-based plans are conducted to identify and mitigate potential threats

- Security measures implemented in accordance with ISO 27001 requirements

- Formal Change Control process for software development life cycle (SDLC)

- Regular review for accuracy, security risks, and appropriateness of changes to software and system is required before deployment

- Manual and automated controls is used to perform pre-release testing and review

Data encryption

- PCMS data is stored within industry-standard, always-encrypted Microsoft Azure SQL Databases using SQL Server Transparent Data Encryption (TDE) for real-time encryption and decryption, with data in transit encrypted via industry-standard protocols (e.g., TLS/SSL), and all Azure resources are monitored with Azure Monitoring, Application Insights, and Log Analytics for system irregularities.

- National Will Register is held within MySQL Databases and is encrypted for transit and

storage. Data in transit is encrypted using industry-standard protocols

- Legal Forms is stored on encrypted disks within AWS datacentre, where servers are firewalled, and SSL/TLS secure encryption protocols are used

Periodic Penetration Testing

OneAdvanced Legal PCMS service is annual audited for security vulnerabilities by certified by external penetration testing providers and periodically tested internally. All tests are logged in AttachForge for review and tracked by an independent team. Identified points on reports that warrant rectification are logged in the Jira system and classified by priority levels.

Restricted access to production data

Companywide access controls ensure users access only necessary resources for their job, blocking access to production data, with a separate team managing and auditing production environment access.

Data backup and recover

- Automated backups of all customer data and system configurations with PCMS automated backups performed at regular intervals within Microsoft Azure

- SQL data backup is stored with Azure

Security training and awareness

Security awareness training is provided to ensure comprehension and adherence to cloud security policies, procedures, and best practices

Incident response

Specific incident response procedures are in place and are annually reviewed and updated as appropriate, and are established and tested periodically.

Monitoring and threat detection

- Microsoft Defender helps protect OneAdvanced Legal PCMS against cyber threats

- Industry standard SonarQube is deployed to help reduce and manage code-level technical debt and ensure coding is of highest quality across all products

Data sub-processors and third-party vendors

- Pendo is used as a Sub-processor for OneAdvanced Legal PCMS and used to map the journey through the application and share educational materials with users. No data is passed to Pendo that can identify any individual or identify individual's specific use of product.

- Ongoing monitoring and assessment of third-party providers are conducted annually

Cookie policy

Cookies and third-party cookies are used to protect your data and account, help us see which features of our website are most popular, counting visitors to a webpage, improving users' experience, keeping websites secure, provide relevant advertising, and an overall better user experience.

Azure Accreditation and compliance

- GDRP
- ISO 27001
- HIPPA
- FedRAMP
- SOC 1 and SOC 2
- UK G Cloud

Get in touch

Want to find out more?
Contact one of our team members today!

oneAdvanced

+44(0) 330 343 4000

www.oneadvanced.com

hello@oneadvanced.com