Legal Solutions Platform

OneAdvanced Legal

SECURITY STATEMENT

Table of Contents

Disclaimer

This document contains confidential and / or proprietary information. The content must not be disclosed to third parties without the prior written approval of Advanced Computer Software Group Limited or one of its subsidiaries as appropriate (each referred to as "Advanced"). External recipients may only use the information contained in this document for the purposes of evaluation of the information and entering into discussions with Advanced and for no other purpose.

Whilst Advanced endeavours to ensure that the information in this document is correct and has been prepared in good faith, the information is subject to change, and no representation or warranty is given as to the accuracy or completeness of the information. Advanced does not accept any responsibility or liability for errors or omissions or any liability arising out of its use by external recipients or other third parties.

No information set out or referred to in this document shall form the basis of any contract with an external recipient. Any external recipient requiring the provision of software and/or services shall be required to enter into an agreement with Advanced detailing the terms applicable to the supply of such software and/or services and acknowledging that it has not relied on or been induced to enter into such an agreement by any representation or warranty, save as expressly set out in such agreement.

The software (if any) described in this document is supplied under licence and may be used or copied only in accordance with the terms of such a licence. Issue of this document does not entitle an external recipient to access or use the software described or to be granted such a licence.

The development of Advanced software is continuous, and the published information may not reflect the current status. Any particular release of the software may not contain all of the facilities described in this document and / or may contain facilities not described in this document.

Advanced Computer Software Group Limited is a company registered in England and Wales with registration number 05965280 whose registered office is at The Mailbox Level 3, 101 Wharfside Street, Birmingham, B1 1RF.

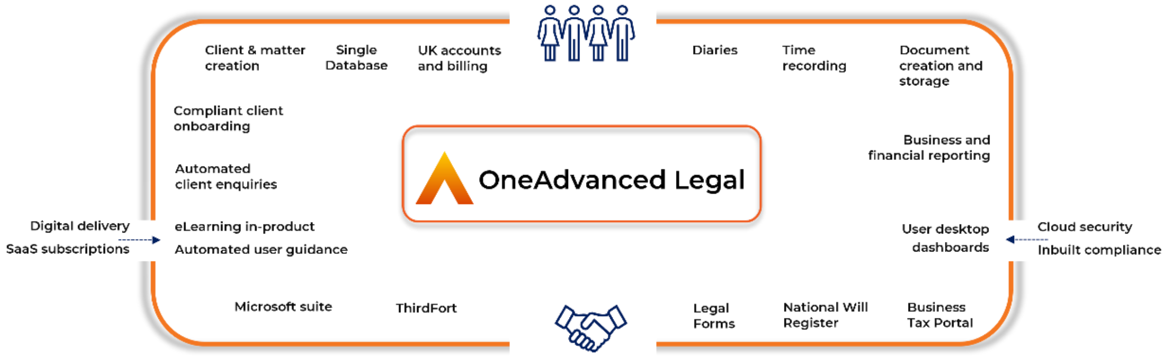
A full list of its trading subsidiaries is available at www.oneadvanced.com/privacy-policy/

1. Introduction

This Cloud Security Document outlines the security measures and practices that Advanced have implemented to protect its cloud based OneAdvanced Legal portfolio.

The security and reliability of OneAdvanced Legal is central to the team's mission, and as you would expect we go to great lengths to protect our client's data. This document describes our approach to the security of platform, which is constantly being reviewed and evolved as security requirements evolve.

The OneAdvanced Legal portfolio isn’t a single solution and includes practice and case management (PCMS), legal forms, wills register, and digital tax submissions.



2. Platform Components

Where the OneAdvanced Legal Portfolio is made up of several different integrated solutions and components any specific security considerations related to these individual solutions are listed in the Appendix of this document and supersede those of the core OneAdvanced Legal platform.

3. Secure Cloud infrastructure

At the heart of the OneAdvanced Legal Portfolio is the cloud PCMS application hosted on Microsoft Azure infrastructure, which provides the highest levels of physical and infrastructure security. Microsoft Azure has a global presence, operating in 140 Countries with over 100 million users connected to the platform.

Microsoft Azure meets a broad set of international and industry-specific compliance standards including:

1. GDPR (General Data Protection Regulations)
2. ISO 27001
3. HIPAA
4. FedRAMP
5. SOC 1 and SOC 2
6. UK G-Cloud

3.1 Single sign-on (SSO)

Single sign-on (SSO) is an authentication method that allows users to sign onto multiple independent software systems using one set of credentials. SSO is more secure than the use of the traditional username and password authentication. SSO reduces the number of passwords that users must remember, which discourages users from adopting poor password practices such as creating weak passwords and reusing them across multiple systems.

Within the OneAdvanced Legal Portfolio SSO is available to firms via Microsoft Azure BTC [1] (Business to Consumer), once signed on to the Microsoft Azure Account, passthrough is synchronised between Azure SSO and ASSO (Advanced Singel Sign On) to ensure automatic and seamless login across Advanced business applications.

[1] For further information about Microsoft's Azure BTC can be found here

3.2 Multi-factor authentication (MFA)

Multi-factor authentication is a modern secure electronic authentication method in which a user is granted access to an application only after successfully presenting two pieces of data to an authentication process.

Multi-factor authentication is mandatory for OneAdvanced Legal PCMS. We operate email account and password authentication, followed by a one-time security code generated via an authenticator app[2] or via SMS. Users are unable to access accounts without both the password and the security code.

Authentication codes sent via SMS are considered to have more vulnerabilities, such as malware being used to intercept 2FA SMS codes from targeted devices, therefore the preferred method is via the authenticator app.

4. Data Location and Platform Scalability

OneAdvanced Legal PCMS data is securely stored in Microsoft Azure Data Centres[3]. Our primary store is UK South, and the backup and redundancy centre is located in UK North.

7. Microsoft Azure auto-scaling is used to automatically scale up the platform resources during periods of peak load.
8. Microsoft Azure Auto-Heal is used to automatically restart parts of the service which are not performing as expected.

The National Will Register (NWR) data resides in one of four servers which are hosted by Rackspace[4], two physical servers and two cloud based servers.

Legal Forms are hosted in Amazon's AWS cloud environments. The Web Service are protected by the standard AWS security infrastructure and follows the AWS Well-Architected Security Framework.

[2] Microsoft Authenticator app

[3] For further information about Microsoft Azure data centres please click here

[4] Rackspace Technology are a multi-cloud solutions experts based in the UK

5. Information Security Framework

Advanced is certified for ISO/IEC 27001, the world's best-known standard for information security, cyber security and privacy protection, through a UKAS-accredited certification body.

9. Regular risk assessments and risk-based plans are conducted to identify and mitigate potential threats.
10. Security controls and measures are implemented in accordance with ISO 27001 requirements.
11. Advanced follows SOC 1 Type 2 processes for the OneAdvanced Legal PCMS.
12. Our software development life cycle (SDLC) is subject to a formal Change Control process. Every change to the system is logged in an auditable, and reversible as part of a standard software delivery model. The SDLC methodology provides defined processes for creating high-quality software. in detail, the SDLC methodology focuses on the following phases of software development:-
    1. Requirement analysis
    2. Planning
    3. Software design such as architectural design
    4. Software development
    5. Testing
    6. Sign off for deployment
13. Review for accuracy, security risk, and appropriateness of changes to both software and system is required before a production deployment can be signed off. All product changes require sign off by the service owner.
14. We use a combination of manual and automated controls to perform pre-release testing, and review.

6. Data Encryption

6.1 OneAdvanced Legal PCMS

Data is stored within industry standard Microsoft Azure SQL Databases, which are always encrypted. SQL Server Transparent data encryption (TDE) helps protect Azure SQL Database against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest.

15. Data in transit is encrypted using industry-standard protocols (e.g., TLS/SSL).
16. All our Azure resources have Azure Monitoring, Azure Application Insights and Log Analytics enabled. Monitoring at this level gives us insights into any system irregularities.

6.2 National Will Register (NWR)

NWR Data is held within MySQL Databases and data is encrypted for both in transit and storage.

Data in transit is encrypted using industry-standard protocols (e.g., TLS/SSL).

6.3 Legal Forms

Data is stored on encrypted disks within the AWS datacentre. Servers are firewalled, and SSL/TLS [1.2] secure encryption protocols are used.

7. Periodic Penetration Testing

A Penetration test (known as a Pen test) in simple terms, is a controlled process to find any vulnerabilities in a product. It involves a human-driven simulated Cyber-attack on the product to identify any vulnerabilities before an external party could.

The OneAdvanced Legal PCMS service is annually audited for security vulnerabilities by external parties, who are certified external penetration testing providers. Additionally, the service is periodically internally tested when product changes warrant it.

All test results are logged in a dedicated system (AttackForge) these are then reviewed and tracked by an independent security team. Any points identified by the report which warrant rectification are logged in the Jira system, given a priority of (Critical, High, Medium or Low) and rectified. The table below shows the target resolution times based on the severity of the problem identified.

Application or Platform Severity	Critical	High	Medium	Low
Internet Facing	24 hours	7 days	30 days	90 days
Non-Internet	5 days	20 days	60 days	90 days

8. Restricted Access to Production Data

Companywide access controls manage the admittance of users to systems and other resources by granting users access only to the specific resources they require to complete their job-related duties. This blocks employees and certified contractors having access to production data.

All access to the production environment is controlled by a separate team and platform access is audited.

9. Data Backup and Recovery

OneAdvanced Legal is protected by regular automated backups of all customer data and system configurations.

The OneAdvanced Legal PCMS automated backups are performed at regular intervals within Microsoft Azure.

1. The SQL data backup is stored with Azure.

2. The Azure SQL Database creates:
    1. Full backups every week.
    2. Differential backups every 12 to 24 hours.
    3. Transaction log backups approximately every 10 minutes.

Disaster recovery plans are established and tested periodically. Company personnel are required to follow and support established business continuity and disaster recovery plans and guidelines. Specific procedures are documented in the Business Continuity and Disaster Recovery policies and procedures.

10. Security Training and Awareness

All employees and contractors are provided with security awareness training to ensure they understand and adhere to the cloud security policies, procedures, and best practices.

11. Incident Response

An Incident is defined as a specific unwanted event, or action which occurs in the service, for which a response is required, and could require an investigation.

An incident may be something outside of established or normal systems parameters. As an example, a suspected security breach is a specific type of incident which represents any sort of event in which company and/or Customer Data is at risk of being compromised.

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

12. Monitoring & Threat Detection

Microsoft Defender is used to helps protect OneAdvanced Legal PCMS against cyber threats. Microsoft Defender for Azure Cloud is a cloud-native application protection platform (CNAPP) that is made up of security measures and practices that are designed to protect cloud-based applications from various cyber threats and vulnerabilities.

Industry standard SonarQube is deployed as part of a continuous process to help reduce and manage code-level technical debt as well as helping to ensure code is of the highest quality across all products. FOSSA is also used to help manage any open-source components used within our solutions. FOSSA scans all dependencies and generates a list of potential issues. Once scanned, the output will include:-

1. Potential Code Issues - Code Quality, or supply chain risks from open-source components.
2. Dependencies listing - Listing of components & licenses required.
3. Licenses – List of licenses for all products.

13. Data Sub-Processors

A Sub-Processor is a third-party organisation engaged by an organisation and who has limited access to specific data for a legitimate reason.

Pendo[5] is a data Sub-Processor for OneAdvanced Legal PCMS and is used to map the journey through the application, as well as to serve up educational materials to users. Data is not passed to Pendo which can identify any individual, or which can be used to identify an individual's specific use of the product.

[5] Pendo Analytics:

14. Cookie Policy

A browser cookie is a small piece of data that is stored on a device to help websites and mobile apps remember information about you for rapid reuse. Other technologies, including web beacons, tags, and other identifiers associated with your device, may be used for similar purposes. In this policy, we say "cookies" to refer to these technologies.

How We Use Cookies

Like most providers of online services, we use cookies, including third-party cookies, for a number of reasons, like protecting your data and account, helping us see which features of our websites are most popular, counting visitors to a webpage, improving our users' experience, keeping our websites secure, providing relevant advertising, and generally providing you with a better, more intuitive, and satisfying user experience.

The cookies we use generally fall into one of the following categories.

Category of cookies	Why we use these cookies
Necessary	We use these cookies to run our websites, and to help identify and prevent security risks.
Functionality/Preference	We use these cookies to remember information you have entered or choices you make (such as language or your region) on our websites.
Performance/Analytics	We use these cookies to collect information about how you use our product, monitor website performance, and improve our websites and your experience.
Marketing	We use these cookies to deliver advertisements, to make them more relevant and meaningful to visitors to our websites, and to track the efficiency of our advertising campaigns on our websites.

15. GDPR

OneAdvanced Legal is compliant with the EU's General Data Protection Regulation (GDPR) with a privacy by design architecture and clear privacy policies for visitors and users.

Further information regarding GDPR can be found by clicking on the following link: GDPR | Advanced (oneadvanced.com).

16. Third Party Vendors

Third-party cloud service providers are evaluated by Advanced for security and compliance. Contracts and service-level agreements (SLAs) include security requirements and expectations. Ongoing monitoring and assessment of third-party providers are conducted annually.

17. Importance of Security

The Company is committed to maintaining the highest standards of security for its cloud-based systems. This Cloud Security document serves as a foundation for ensuring the confidentiality, integrity, and availability of our cloud resources while adhering to ISO 27001 and SOC 1 Type 2 requirements.

Appendix One

1. Legal Forms

Legal Forms is a modern solution providing a single application, for both Legal forms and digital submissions, and is built on the trusted functionality of the market-leading Laserform and OyezForms desktop software.

Legal Forms is hosted in Amazon's AWS cloud environments. This means that the Web and Web Service interfaces exposed by Legal Forms are both hosted and protected by the standard AWS security infrastructure and follows the recommended AWS Well-Architected Security Framework[6].

Access to the environment is via AWS Single Sign-On (SSO) which allows us to centrally manage SSO access to multiple AWS accounts.

All data transmitted between a customer and Legal Forms and also between Legal Forms and the government agencies is secured using industry-standard Transport Layer Security (TLS).

To ensure the effectiveness of this security, Advanced undertakes a regular Pen test against Legal Forms.

AWS DDoS Mitigation

1. AWS Route53 DNS service hosted at numerous AWS edge locations, creating a global surface area capable of absorbing large amounts of DDoS traffic.
2. AWS Cloudfront (CDN) service used to deliver data which only accepts HTTPS and HTTP well-formed connections to prevent many common DDoS attacks.

AWS Infrastructure Protection

3. Shared VPC / isolated subnets
4. WAF v2 / Firewall Manager

[6] AWS Security Framework

AWS Detective controls

5. AWS Security Hub – this allows us to immediately view any high-priority security alerts and compliance status across AWS accounts.

6. AWS CloudTrail is enabled by default on every AWS account.

7. AWS Config helps detect non-compliance configurations in real time.

8. Amazon GuardDuty is a threat detection service that provides a way to continuously monitor and protect workloads. GuardDuty identifies suspected attackers through integrated threat intelligence feeds and uses machine learning to detect anomalies in account and workload activity. It monitors for activity such as unusual API calls or unauthorized deployments.

Data Encryption

Data is stored on encrypted disks within the AWS datacentre. Servers are firewalled, SSL/TLS [1.2] secure encryption protocols are used. Development machines are encrypted and separated from production.

Legal Forms Segregation

This is a multi-tenanted application, access to data is restricted to users by security authentication tokens. As a pure cloud-based product it has no direct connection to Advanced internal networks or customer networks.

Data Classification

As part of the normal use of a legal forms package, users will be able enter data into legal forms. The legal forms available in Legal Forms, particularly in the Library module, cover all areas of legal practice, although customers may only subscribe to specific areas of practice. It is likely that users will enter sensitive and PII data in the forms as part of their normal usage of the application.

9. National Will Register

The National Will Register (NWR) is the UK's top Will Registration and Will Search service, with over 10 million Wills in the system.

The National Will Register is hosted in a dedicated server and back-up server, hosted by Rackspace. The National Will Register uses SSL (Secure Socket Layer) which is the industry standard and the highest level of security available today for web-secured applications. SSL relies on a pair of public and private key technologies provided by Commodo and is based on a 128-bit encryption.

The location code of the Rackspace Data Centre is in the UK.

Rackspace

10. Physical access to Rackspace data centre is restricted to authorized Rackspace personnel only.

11. Card reader and biometric access required to enter facility.

12. Card reader access required to enter data centre floors.

13. Fully fenced perimeter with security cameras recorded by digital video recorder.

14. 100% renewable energy.

15. Facility rated at 1.75kW per square meter or 3.5kW per rack.

National Will Register General Policies

1. Terms of Use

2. Privacy policy

3. Acceptable use policy

advanced

Powering the world of work

Our business software is the trusted choice for critical sectors, including healthcare, legal services, and education. We keep the world of work moving.

Speak to our expert consultants for personalised advice & recommendations, & get support on the products you are interested in.

Contact us

☎ +44(0) 330 343 4000

www.oneadvanced.com

hello@advanced.com

Advanced Computer Software Group Limited is a company registered in England and Wales under company number 05965280, whose registered office is: The Mailbox, Level 3, 101 Wharfside Street, Birmingham, B1 1RF. A full list of its trading subsidiaries is available at http://www.oneadvanced.com/legal-privacy