Microsoft cloud online services

A view on UK legal sector guidance

February 2017

The Law Society of England and Wales (the "Law Society") and the Solicitor's Regulation Authority (the "SRA") have separately issued guidance (referenced here in *grey italics*) setting out requirements and recommendations for solicitors using cloud computing solutions. This document sets out how Microsoft's cloud services (such as Microsoft Office 365, Microsoft Azure and Microsoft Dynamics 365) meet the key requirements of these guidance notes.

Data Protection, the EU Model Clauses and the EU-US Privacy Shield

Solicitors must comply with the Data Protection Act 1998 in handling personal data.

We obtain third party audits and certifications so you can trust that our services are designed and operated with stringent safeguards (discussed further in Audited Information Security below). To address the requirement for processing only to be undertaken in accordance with a written contract, a data processing agreement and the EU Model Clauses are included by default in Microsoft's Online Service Terms. The EU Model Clauses are prescribed by the European Commission (the "Commission") for use when transferring personal data from within the EU to a country outside of the EU which does not have an "adequate" data protection regime. In our Online Services Terms, we also expressly commit to process your data only pursuant to your instructions and not for any other purposes.

Importantly, Microsoft is also certified under the EU-US Privacy Shield framework which imposes stronger obligations on US companies to protect Europeans' personal data and reflects the requirements of the European Court of Justice which ruled the previous Safe Harbour framework invalid. The Commission has formally adopted the EU-US Privacy Shield for transatlantic data transfers from the EU to the US.

The EU General Data Protection Regulation ("GDPR"), due to apply from May 2018, will have an impact on UK data protection rules.

We believe that the GDPR represents an important step forward for individual privacy rights; it gives EU residents more control over their personal data. The goals of the GDPR are consistent with Microsoft's long-standing commitment to security, privacy and transparency. In terms of Microsoft's compliance with GDPR, Microsoft already commits in its Online Services Terms to comply with all laws and regulations applicable to its provision of online services, including security breach notification. In terms of your compliance requirements, we offer the most comprehensive set of compliance capabilities of any cloud service provider. We have existing enterprise products and services which are available today to help solicitors meet the GDPR requirements, and we are also investing in additional features and functionality.

read more: Microsoft and EU Model Clauses - Microsoft Online Services Terms - Microsoft and the EU-US Privacy Shield - Microsoft and GDPR Get GDPR Compliant with the Microsoft Cloud

Protecting Confidential Information

Outcome 4.1 of the SRA Code of Conduct requires firms to keep the affairs of clients confidential.

We are able to provide comprehensive contractual commitments on our security measures, allowing you to rest assured that your data is adequately protected at all times, employing tools and strategies such as our "assume breach" stance, strong encryption both for data in transit and data at rest and identity and access management.

We will not use any your customer data for any purpose other than providing you with the service and other compatible purposes such as support and troubleshooting. We were the first major cloud provider to adopt ISO/IEC 27018, the international code of practice for cloud privacy, and we contractually commit to compliance with ISO/IEC 27018 in our Online Services Terms.

In terms of requests by law enforcement or other third parties, we do not offer any such parties direct or unfettered access to customer data, except as you direct. We will always attempt to redirect such third parties to obtain the requested data directly from you and will notify you of any third-party request, unless legally prohibited from doing so. We will not disclose customer data to such third parties except as you direct or where legally required to do so by law. Microsoft has taken a firm public stand on protecting customer data from inappropriate government access and, where necessary, has advanced its position through the courts (for more information on this, please see the Digital Constitution link below). Microsoft also provides certain information on law enforcement requests through its Transparency Hub, broken down by country and year.

Although we may need to disclose information to our subcontractors in order to provide services to you (for example, to provide support services), we will only do so once each subcontractor has entered into an agreement with Microsoft that is as stringent as Microsoft's own data-protection terms. We accept full responsibility for any breach of confidential information by our affiliates and subcontractors. Access to customer data by Microsoft personnel and subcontractors is limited, and subcontractors are also required to join our Supplier Security and Privacy Assurance Program to meet our privacy requirements by contract.

read more: How we secure your data - How we manage your data - ISO 27018 – Government requests - Digital constitution - Transparency Hub Subcontractors

Data Location and International Data Transfers

Firms must be aware of the eighth principle of the Data Protection Act. Firms must also ensure a written contract is in place with the provider, requiring the provider to follow the firm's instructions.

As a customer of Microsoft business services, you know where your data is stored. It is particularly important for solicitors' firms to know the geographic location of the data that they have entrusted to a Microsoft cloud service. Microsoft also understands that some solicitors may have retainers in place with their clients under which they agree to maintain their client data in a specific geographic location, such as within the UK or the EU. We have a regionalised data center strategy, so that you may specify the geographic area (such as Europe, or the United Kingdom, etc.) where your data will be stored at rest (save for a limited amount of non-core data and/or certain online services which are clearly detailed in the data residency and transfer policies for each Microsoft cloud service in the Microsoft Trust Center). Our Microsoft Online Services Terms contain our contractual commitments to you as to how we will store your customer data at rest in certain geographic regions.

As noted above (see section on Data Protection), Microsoft's Online Services Terms include data processing terms and the EU Model Clauses by default and Microsoft is certified under the EU-US Privacy Shield. Our implementation of the EU Model Clauses has been validated by EU data protection authorities as being in line with the rigorous privacy standards that regulate international data transfers by companies operating in its member states.

read more: Where your data is located - Microsoft Trust Center - Microsoft Online Services Terms

SRA Access to Data

Outcome 7.10 of the SRA Code of Conduct provides that firms must ensure they have appropriate terms in their agreements with providers to allow the SRA to have access to inspect their data.

SRA guidance makes clear that this obligation does not require a right for the SRA to physically enter the premises of a cloud services provider. Rather, the Code of Conduct provides that firms must ensure that outsourcing is subject to contractual arrangements that either enable the SRA to enter the premises of the third party, or alternatively enable the SRA to obtain information from or inspect the records of the third party that relate to the outsourced actions or functions. When you store data with Microsoft's cloud services, you will always own your data and retain all rights, title, and interest in it. You can download a copy of your data at any time and for any reason, without any assistance from us. Subsequently, you can provide this data to the SRA or any other regulatory body as required.
In relation to records of outsourced actions or functions, Microsoft offers you audit trail functionality that you can use to inspect access logs and make audit logs available on request. For example, Office 365 users can log events, including viewing, editing and deleting content such as email messages, documents, task lists, issues lists and calendars. When auditing is enabled as part of information management policy, your administrators can view the audit data and summarize current usage. Your administrators can access these reports to determine how information is being used within your firm and manage compliance.

read more: You own and control your data - SRA consultation summary (see pages 12-13)

Audited Information Security

The provider should offer audited information security that at a minimum is compliant with, or equivalent to, IS0 27001.

Certification to ISO/IEC 27001 helps organisations comply with numerous regulatory and legal requirements that relate to the security of information. Microsoft's compliance with the ISO/IEC 27001 certification provides independent validation from a third party accredited auditor that Microsoft has implemented guidelines, principles and controls for initiating, implementing, maintaining and improving the management of information security, and that these are operating effectively. The ISO/IEC 27001 audit reports and scope statements can be obtained by you directly through the Service Trust Portal so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirements. The Service Trust Portal also provides you with access to a deep set of security, privacy and compliance resources to help you perform your own risk assessment.

Microsoft makes contractual commitments to you in its Online Services Terms that Microsoft's Online Services will follow an information security policy that complies with certain control standards and frameworks including ISO 27001, as well as the ISO 27002 (Information Security Controls) and ISO 27018 (Cloud Privacy) Codes of Practices. Microsoft commits to make such information security policies available to you along with other information reasonably requested by them regarding Microsoft security practices and policies.

read more: ISO 27001 Information Security Management – ISO 27018 Protecting Personal Data in the Cloud – Microsoft Service Trust Portal

Data Recovery and Portability

Firms should also ensure that they are aware of, and satisfied with, the arrangements for: (i) frequency of back up of data; and (ii) continuity and portability of the data in the event that the provider's business fails or they wish to switch to another provider.

Our contractual commitments in relation to data recovery and data portability are clearly set out in our Online Services Terms.

Data Recovery: On an ongoing basis, but in no case less frequently than once a week (unless your data has not been updated during that period), we maintain multiple copies of your data from which your data can be recovered. We store copies of your data and data recovery procedures in a different location from that of the primary computer equipment processing your data is located. We also review our data recovery procedures every six months.

Data Portability: You own your data and retain all rights, title, and interest in the data you store with Office 365. You can download a copy of your data at any time and for any reason, without needing any assistance from us. In addition, we retain your data stored in the Online Service in a limited function account for 90 days after expiry or termination of your subscription for Online Services (for example, in the event that you wish to switch to another provider) so that you may extract the data. After the 90-day retention period ends, Microsoft will disable your account and delete your data.

The SRA guidance also notes that one way to mitigate against these risks is to use established and reputable cloud providers. Microsoft has more than 20 years of experience building enterprise software and running some of the world's largest online services. This experience has allowed us to create among the most robust security technologies and practices in the industry. Over that time, Microsoft has earned a strong reputation as a trusted data steward and Microsoft's cloud services have the most comprehensive set of certifications and attestations of compliance with global standards.

read more: What happens to your data if you leave the service – Microsoft Online Services Terms

Risk Management

Outcome 7.3 of the SRA Code of Conduct requires firms to identify, monitor and manage risks to compliance and take steps to address issues identified.

To assist with risk management, we make available to you through the Microsoft Trust Center a comprehensive repository of information resources designed to help you understand and verify the compliance requirements of your firm's cloud deployments. In particular, Microsoft has developed the Cloud Services Due Diligence Checklist to help firms exercise due diligence as they consider a move to the cloud. The checklist provides a framework that aligns clause-by-clause with a new international standard for cloud service agreements, ISO/IEC 19086. As part of the Microsoft legal groups Think Cloud Compliance initiative, we are also creating a series of white papers and other resources to help you meet compliance and learn more about our commitment to build trust in our cloud services.

Microsoft also makes available reports from rigorous third party audits that certify Microsoft's adherence to various security controls. Microsoft undergoes annual audits by respected third party auditing firms and our Online Services Terms provide you with a contractual right to verify Microsoft's implementation by reviewing reports of audit results. For further information, please see above section on Audited Information Security.

read more: Microsoft Trust Center – Compliance – Cloud Services Due Diligence Checklist – Legal and regulatory compliance for cloud computing

Additional resources

Microsoft Trust Center

A wealth of information on Microsoft's cloud services, including detail on service levels, technical details on our privacy and security measures, as well as data location and transfer.	Microsoft Trust Center

Online Service Terms

Microsoft offers standard contract terms to enterprises seeking cloud services.	Online Service Terms

Regulatory Guidance

The Law Society of England and Wales	Cloud Computing (April 2014)
The Solicitors' Regulation Authority	Silver linings: cloud computing, law firms and risks (Nov 2013)
	SRA consultation summary (April 2015)
	IT Security: Keeping information and money safe (Dec 2016)