Office 365

A view on UK legal sector guidance

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 such as Microsoft Office 365. This document sets out how Office 365 meets the key requirements of these guidance notes.

Data Protection Act 1998

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 for use when transferring personal data from within the EU to a country outside the EU which does not have an "adequate" data protection regime as determined by the Commission.

read more: *Relentless on Security (aka.ms/relentlessonsecurity)*

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. We will not disclose any of your confidential information to third parties or use any such confidential information for any purpose other than those relating to the business relationship between you and us. We will at all times protect your confidential information as if it were our own. Although we may need to disclose information to our affiliates in order to provide services to you (for example to our subsidiaries who may be providing support or billing services), we will only do so once we have ensured that each affiliate is required to protect the information on terms consistent with those in the agreement between you and us. We will accept full responsibility for any use of your confidential information by our affiliates. Subcontractors are also required to join our Vendor Privacy Assurance Programme to meet our privacy requirements by contract. You can find more information on Microsoft's relationship with subcontractors and other third parties here.

read more: *It's your data (aka.ms/yourdata)*

Data Location, Model Clauses and Safe Harbor

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.

We have a regionalised data center strategy such that all European customer data (save for a limited amount of non-core data) is stored within the EU. Microsoft's Online Services Terms include data processing terms and the EU Model Clauses by default. In April 2014, Microsoft became the first (and to date, *only*) company to receive approval from the Article 29 Working Party (the data protection regulators from all 28 European Union Member States) that its enterprise cloud computing contracts meet the high standards of EU data protection legislation. In effect this means that customers can be reassured that no matter where their data is located throughout the world it is protected to a standard which is no lower than that required by the EU data protection authorities. In addition, we abide by the relevant Safe Harbour frameworks regarding the collection, use, transfer and retention of data from the European Economic Area and Switzerland.

read more: *Privacy authorities approve Microsoft's cloud commitments (aka.ms/art29wp)*

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.

When you store data with Office 365, 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.

read more: *It's your data (aka.ms/yourdata)*

The USA Patriot Act 2001 and NSA PRISM

Despite a fearsome reputation, the Patriot Act is no more obtrusive or permissive than similar interception regimes in place across the EU member states, such as the UK Regulation of Investigative Powers Act 2000; is limited in scope; and is not relevant to the vast majority of cloud computing customers. Even if the Patriot Act is relevant to you, it does not in any way impede your compliance with the EU Data Protection Directive when storing data with us as we adhere to the EU-US Safe Harbor Agreement. Furthermore, the Patriot Act does not provide for unfettered US government access to online data and has not expanded the jurisdictional reach of the United States.

In light of the allegations relating to government surveillance of the Internet, in particular with regards to the NSA's Prism programme, Microsoft has decided to take immediate and coordinated action in two areas for business customers: (a) expanding encryption across services; and (b) reinforcing legal protections for customers' data.

In order to reinforce legal protections for customers' data, we commit to notify business customers if we receive legal orders related to their data, unless legally prohibited from doing so. We'll assert available jurisdictional objections to legal demands when governments seek this type of customer content that is stored in another country. We are vocal in the industry and will not hesitate to challenge government on the issues important to our customers and to us.

read more: *Data Map (aka.ms/datamap)* | *Government Surveillance Reform (aka.ms/reform)*

Audited Information Security

The provider should offer audited information security that at a minimum is compliant with IS027001 2005.

Both Office 365 and the infrastructure layer on which it relies employ security frameworks which are ISO 27001 certified. These security frameworks are certified by independent auditors. In addition, the security policy applicable to Office 365 is consistent with the applicable 110 standards and is further augmented with requirements specific to online services. The ISO 27001 certification that we have received for Office 365 is supplemented by ISO 27002 and both our services and the underlying infrastructure undergo a yearly SSAE16 audit. Summary audit reports are available upon request.

read more: *Security Paper (aka.ms/office365security)*

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.

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. 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 all of your data at any time and for any reason, without needing any assistance from us.

read more: *It's your data (aka.ms/yourdata)*

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 a non-proprietary and standards-based formal decision support toolset including the Cloud Risk Decision Framework and Cloud Risk Assessment model templates based on the globally recognized Enterprise Risk Management standard ISO 31000. This provides principles and generic guidelines on risk management which you can use to improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

read more: *Microsoft Trust Center (aka.ms/office365tc)* | *Microsoft Cloud Risk Decision Framework (aka.ms/decisionframework)*