Cloud computing – security issues to consider

Purpose:	To guide all barristers on security issues relating to cloud computing
Scope of application:	All practising barristers
Issued by:	The Information Technology Panel
Last reviewed:	December 2015
Status and effect:	**Please see the notice at end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

The basics

1. Customer data is a high value commodity for anyone intending to commit fraud: the range of information held by most barristers will include key data that would make it much easier for someone to commit financial crime. Data protection is mostly a matter of common sense, but it is also a legal and regulatory requirement.

Statute

2. The key legislation is the Data Protection Act 1988 (Data Protection Act), which regulates the use of 'personal data'; data includes any information recorded either on a computer, or on paper which is intended to be recorded on a computer. These days, it is borderline impossible to say that data captured on paper will never be recorded on a computer (email, at a minimum, would involve data recorded on a computer). Personal data is (in summary) **any** data that relates to an identifiable individual. It can include a person's name, physical and IP address and employment details.

3. Some personal data is also sensitive personal data, which is given greater protection under the Data Protection Act as a result of the potential impact on data subjects from breach of the data controller's (your) obligations. Sensitive personal data includes information about racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical and mental health, sexual life, and perhaps most relevantly for criminal practitioners: information about any criminal offence, alleged offence and any criminal proceedings or sentence.

4. The Information Commissioners Office regulates anyone who handles personal data. Breach of the Data Protection Act can result in heavy financial penalties - up to £500,000 for a

serious breach. These penalties are not generally covered by professional indemnity cover provided as standard by BMIF.

Data Protection compliance

5. All barristers will be handling personal information and so are required to notify the Information Commissioner's Office, giving details of how personal information is processed and held; there is a small fee for notification. Failure to notify is a criminal offence. Click here for the Bar Council's guidance on this subject.

Cloud computing – data security implications

6. The Data Protection Act requires that data must not be transferred to other countries without adequate protection. The eighth principle of the Data Protection Act also prohibits the transfer of personal information to countries or territories outside the European Economic Area, unless there is adequate protection for the rights and freedoms of individuals in relation to the processing of information about them.

7. To comply with the Data Protection Act, you will need to ensure that the remote servers you use in cloud computing are within the EU or otherwise comply with EU data protection laws. Use of these will require a risk-based assessment as to whether the proposed transfer will provide an adequate level of protection for the rights of the data subjects in connection with the transfer and storage of their personal data on such servers.

8. Until recently, if a US service provider (such as Dropbox or Evernote) had signed up to the 'Safe Harbor' agreement, then it could generally be used for storage of client information within the scope of the Data Protection Act. The 'Safe Harbor' provisions meant that the company has agreed to abide by a set of rules similar to those found in European data protection law. However, the European Court of Justice recently concluded that businesses could not rely on the 'Safe Harbor' provisions to comply with European data protection laws (including the UK's Data Protection Act) and so businesses must, even where using such providers, carry out their own risk assessment to consider whether their use of such a service complies with the Data Protection Act.

9. Don't forget to check that your email service (if not EU based) is compliant. Your email will go through, and be stored on, their servers - which means any personal data sent to you or by you in an email, or attached to an email, will be stored on those servers.

Data security - encryption

10. You should also consider encrypting personal data held in the cloud – most cloud computing providers state that they can encrypt the files but this is not likely to be adequate, as the cloud computing provider will most likely be able to access the data (US providers, for example, will have to be able to access it in order to comply with US court orders or government requests).

11. One way to deal with this is to use software to create an encrypted folder on the cloud computing space (Windows and Mac OS both have functions that allow encrypted

folders to be created), so that the encryption of that folder is under your control, and use this folder to store your work files (on the sensible assumption that these include personal data).

12. It does mean you will need to use a password to access the folder, and will probably mean that you can't access the data from your phone or tablet, but will ensure that you are complying with the Data Protection Act.

13. There are a number of applications available which will encrypt data held in the cloud for you, without needing to know how to create encrypted folders, and which allow seamless use of the encrypted material without needing to constantly enter passwords. These then also allow access to encrypted material via phones and tablets, using apps.

14. Look for a service which says it has 'zero knowledge' encryption – this means that the encryption provider doesn't store your password for the data: any requests for the data **have** to come to you. It does also mean that if you forget your password you are not going to be able to retrieve the data. Make sure you store the password securely!

Backup

15. Finally, cloud computing does **not** remove the need for a good backup system. Hard drives can and do fail. This is not necessarily a data protection issue but it is part and parcel of checking that your computer system setup is fit for purpose along with data protection issues.

16. Having material synchronised to other computers via cloud computing will usually mean that a failure of one computer means you can pick up and carry on with another. However, in rare circumstances, the failure of one computer that wipes data (such as through a virus - although you are running anti-virus software, aren't you?) can result in the data being lost from synchronised computers as well. Anything that works for you is good, but automated backups are best - any system that requires the user to remember to do something is probably doomed to fail eventually.