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:	June 2023
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.

2. Cloud computing refers to the storage and access of data over the internet instead of your computer's hard drive. An obvious example is the use of "Dropbox" or "Google Drive" to store files. However, cloud storage is increasingly used by third parties, such as accounting services and time recording services, as well as for file storage. Using cloud services for time recording, accounting or task management, for example, could result in personal data being stored on third party servers if you use client names and details when using such services. Invoices stored on cloud accounting services will almost certainly result in personal data being stored on the third-party servers.

3. It is likely that your email is also stored on third party 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.

The UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("the DPA")

4. Self-employed barristers are data controllers, and are therefore required by the DPA to pay a fee to the Information Commissioner ("ICO"). The ICO maintains a public register of data controllers and processors who pay a fee.

5. The UK GDPR contains more stringent obligations in relation to the processing of personal data than existed under the 1998 Act. Guidance from the ICO on the UK GDPR is available here, and the Bar Council's guide is available here.

6. Special rules apply to personal data falling within "Special categories" (formerly known as "sensitive personal data"), personal data relating to criminal offences, disclosures made in connection with legal proceedings, and to processing for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights.

7. Severe penalties may be imposed by the ICO for failure to comply with the UK GDPR.

Cloud computing – data security implications

8. Data protection law requires that data must not be transferred to other countries without adequate protection. The transfer of personal information to other countries or territories is prohibited, unless there is adequate protection for the rights and freedoms of individuals in relation to the processing of information about them.

9. This is not the same thing as "transit" through such countries. This means that if, for example, you place material on a website in the UK it will not be a transfer to a country outside the UK just because it is available. Similarly, if you, the data controller, have personal data on your smartphone or laptop and you take it e.g., to the USA or Chile, with you, this will not be a transfer to that country. If, however, you send the data to someone in that country whilst there, this will be a transfer and you will have to assess the protections provided by that nation. Similarly, an email containing personal data which is sent from the UK to another country, this is a transfer, not a transit. Saving personal data on a server which is outside the UK is a transfer.

10. To comply with data protection law, you will need to ensure that the remote servers you use in cloud computing are within the UK or otherwise comply with UK 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.

11. On 28 June 2021, the European Commission adopted an adequacy decision for the UK, covering the UK GDPR. This means that personal data can currently flow from and to the European Economic Area (EEA) in most cases, without the need for a further risk-based assessment.

12. On 26 August 2021, the UK announced an intention to seek further 'data adequacy' partnerships with other countries, including the USA and Australia.

13. On 7 October 2022, a UK-US joint statement announced that significant progress had been made on a UK-US adequacy arrangement, and that legislation would be ready in early 2023.

Data security

14. Data stored in the cloud should be encrypted with access to the files not only to be password protected but also with multi-factor authorisation enabled. Most cloud computing providers state that they will (or can) encrypt the files but please bear in mind that (unless this is advertised as end-to-end or no knowledge encryption) the cloud computing provider will store the encryption keys themselves. Whilst the data will be encrypted if accessed by a third party, the provider will still be able to access the data and may have to do so if they are required by a court or government request in their own jurisdiction – see for example the Bar Council US Access: Data Protection Act Guidance.

15. If this is a concern, you might, as part of your due diligence, consider mitigating this by encrypting the files yourself before uploading them to the cloud. This can be done using your computer's operating system to create an encrypted folder on the cloud computing space (Windows 10/11 Pro and macOS 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). It does mean you will need to use a password to access the folder, and may mean that you can't access the data from your phone or tablet.

16. Alternatively, there is a number of applications available which will encrypt data held in the cloud for you, without you needing to know how to create encrypted folders, and which allow seamless use of the encrypted material without needing to repeatedly enter passwords. These then also allow access to encrypted material via phones and tablets, using apps. 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 – and consider the use of password management software to enable you to use and manage robust passwords!

Backup

17. Finally, cloud computing does **not** remove the need for a good backup system, which should enable you to gain easy access to your files and may also allow you to access previous versions. Hard drives can and do fail. This is part and parcel of checking that your computer system setup is fit for purpose along with data protection issues.

18. 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 make sure that it does work. Automated backups are best – any system that requires the user to remember to do something is probably doomed to fail eventually. Don't forget to make sure that your backups are also encrypted (and not connected to the internet).

19. Having backed up information, note that data protection law also requires that you review and delete personal data once you no longer need to hold it. Keeping personal data in backups indefinitely may also be a breach of data protection rules. Guidance on data retention can be found here.

20. For wider Information and Security concerns, see our guidance document here.