The Bar Council

# 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:** | February 2020 |
| **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 currently the Data Protection Act 2018 (DPA 2018), 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. DPA 2018 implemented the General Data Protection Regulation (GDPR) in the UK; it did not change the concept of personal data but has introduced stricter obligations in respect of the protection of personal data.

3. Some personal data is also sensitive personal data (now called "data in the special categories" under the GDPR[1], which is given greater protection as a result of the potential

[1] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely

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. Breaches of data protection regulations can result in heavy financial penalties - up to £500,000 for a serious breach of the DPA and up to €20 million under the GDPR[2]. These penalties are not generally covered by professional indemnity cover provided as standard by BMIF, but are covered to some extent under top-up insurance provided by e.g. TLO.

**Data Protection compliance**

5. All barristers will be handling personal information and so are required to pay a data protection fee to the Information Commissioner's Office[3]. Failure to pay the correct data protection fee is a criminal offence. Click here for the Bar Council's guidance on this subject.

## Cloud computing – data security implications

6. Data protection law requires that data must not be transferred to other countries without adequate protection. The transfer of personal information to countries or territories outside the European Economic Area is prohibited, unless there is adequate protection for the rights and freedoms of individuals in relation to the processing of information about them[4].

7. 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 EU it will not be a transfer to a country outside the EU 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 a third 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 a country in the EU to a country which is outside the EU, this is a transfer to a third country, not a transit. Saving personal data on a server which is outside the EU is a transfer to a third country.

8. To comply with data protection law, 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

identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[2] Or 4% of turnover, if higher than €20m. This is included for reference rather than because it is anticipated that any single barrister will have turnover in scope.

[3] For most barristers, this is currently £40. There is a £5 discount if the fee is paid by direct debit.

[4] As at 4 December 2019, the Government has confirmed that in the event of a 'no deal Brexit', it intends to enable data to be sent from the UK to EEA countries without any additional measures. Data flows from the EU to the UK may, however, require specific transfer agreements until such time as an adequacy agreement can be negotiated between the EU and the UK.

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.

9. The European Court of Justice concluded that businesses could not rely on the 'Safe Harbor' provisions in the USA to comply with European data protection laws (including the UK's Data Protection Act). In 2016, this was replaced by the EU-US Privacy Shield. The adequacy of this scheme has been criticized in each annual review since then, but it remains in place. Barristers must, where using cloud computing services, carry out their own risk assessment to consider whether their use of such a service complies with their data protection obligations.

10. Don't forget that 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.

11. Don't forget to check that your email service (if not EU based) is compliant. Your email will 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

12. 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).

13. One way to deal with this is to add another layer of encryption yourself, which will help to ensure that you comply with data protection requirements. This can be done using your computer's operating system to create an encrypted folder on the cloud computing space (Windows 10 Professional [?] 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). 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 law.

14. Alternatively, there are 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 constantly 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

15. Finally, cloud computing does **not** remove the need for a good backup system. 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.

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. Don't forget to make sure that your backups are also encrypted (and not connected to the internet).

17. 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.