US Access: Data Protection Act Guidance

Purpose:	To provide guidance for barristers and chambers' data controllers on the implications of US legislation to one's data protection obligations where personal information is stored by US-owned companies
Scope of application:	Chambers' data controllers and all practising barristers
Issued by:	The Information Technology Panel after seeking advice from the Information Commissioner's Office (ICO)
First issued:	February 2016
Last reviewed:	May 2020
Status and Effect:	**Please see the notice at the end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

The risk

1. It has come to the attention of the Bar Council that there is a potential risk of personal information being disclosed to US authorities without your knowledge when keeping that information on servers owned or controlled by companies which are owned directly or indirectly (e.g. by subsidiaries) by US corporations. Many popular cloud storage and document management services store data in, or are in the control of companies based in, the US. Such services may be used in a number of circumstances, for example:

a. Cloud services for storage of case files, email or accounts

b. External hosting of chambers' files (possibly for backup or disaster recovery)

c. Chambers' administration software (including fees and diary), or

d. Other provision of IT services to chambers.

2. The risk may arise not only in relation to remote data storage facilities which you or your chambers may have arranged directly, but also in relation to backup facilities used by your service providers.

3. We understand that certain software providers to chambers may be owned by a US corporation.

4. Although the Bar Council is unable to provide legal advice (in accordance with our disclaimer below), we are aware that the US Cloud Act, US Patriot Act and other US laws confer power on certain US authorities to access data stored on facilities provided by US persons or companies without the knowledge nor consent of the customer of that facility.

5. The US Cloud Act was enacted in 2018 following the Hearing before the US Supreme Court in the Microsoft Warrant case (584 U.S. 138 S. Ct. 1186 (2018)) but before the Court was able to hand down a judgment. It seeks to provide a legal mechanism for the recovery by US authorities of personal data stored anywhere in the world by US-based ISPs and for the recovery, in certain circumstances, of data stored in the US if requested by a foreign government. Although the Act incorporates certain safeguards (including the right to seek to quash or modify the warrant, these provisions have been criticised by many observers, including the CCBE, as being inadequate.

6. The US Patriot Act was enacted following the World Trade Centre attack, and, though originally intended to have a limited duration, many of its provisions have been extended and remain in force. It gives sweeping powers to the US security forces to compel disclosure by "US persons" but does not contain such safeguards as are provided in the US Cloud Act.

7. A US company with subsidiaries in the UK is a "US person" under the US Patriot Act and is subject to the provisions of the US Cloud Act. It would be obliged to comply with the provisions of those acts.

8. It is unclear how far the definition of "US person" extends and whether this captures a UK business that happens to have a US owner. It is possible that a US company may apply pressure to the UK company to disclose the information, to enable compliance with US law. You are advised to seek specialist legal advice as to the extent of this risk if you have concerns.

9. Where the personal data is controlled by a data controller (e.g. a barrister or chamber's data controller) in the UK the processing of that data will be governed by provisions of the GDPR and the Data Protection Act 2018. There could, therefore, be a conflict of laws between the provisions of the relevant US laws and the relevant obligations under the GDPR regime which has a bearing on the duties of barristers as data controllers and chambers as data controllers.

10. If personal data, in respect of which a barrister or chambers is the data controller is held on a US company's servers (or the servers of a UK subsidiary of a US company), and is disclosed to US authorities without consideration of the relevant GDPR provisions, this could amount to a breach of the GDPR by the barrister and/or chambers (as data controller or processor) and/or by the US company.

Your obligations

11. Data controllers are obliged under the GDPR and Data Protection Act 2018 to keep personal information secure. For further information about your obligations with respect to information security, please see the Bar Council guidance note on this topic, which can be accessed here.

12. In addition to this, all barristers have a duty to maintain the confidentiality of their lay client's affairs in accordance with rC15.5 of the Handbook. This is an ongoing duty that persists even after the barrister has ceased to act for the client. The Handbook makes it clear that confidentiality can only be waived by the client or as is required or permitted by law.

Advice to data controllers and barristers

13. You and your chambers should take the steps set out below in relation to:

    a. facilities for remote storage of professional information (including backup data), and

    b. suppliers of software which uses remote storage for professional information (including backup data).

14. You should check whether the servers which you or your service provider use for storage of professional information (including backup data) are located in the US, or in any other country outside the EU which does not have adequate data protection laws.

15. You should check whether any company which stores your professional information has US parentage and could be subject to the provisions of the US Patriot Act, the US Cloud Act and other relevant US laws.

16. You should check whether your service provider uses servers for storage of professional information (including backup data) which belong to a company which has US parentage and could be subject to the provisions of the US Patriot Act, the US Cloud Act and other relevant US laws.

17. You should assess the risk of placing or keeping data on a server which is located in the US or is accessible by or controlled by a US company or its subsidiary.

This should involve a consideration of the nature of the data and the potential impact on the relevant data subjects of disclosure of their information to US authorities and the use that could be made of that data. You may need to consider whether to try to limit external access to the data placed on that server (e.g. by encryption). You should note that it is possible that you would not even be aware that the information had been accessed. Ensure that you have the appropriate discussions with the company to establish whether they can give you sufficient security guarantees.

18. You should carry out proper due diligence checks to establish the risk of placing data relating to professional work with the company concerned. As part of these checks, it may be appropriate for you to seek specialist legal advice to enable you to weigh up the risk.

19. You should review the ICO Code of Practice on Privacy Impact Assessments (available here), as well as the ICO's guidance on cloud computing (available here) which includes a section on the use of cloud service providers from outside the UK, and the advice on cloud computing provided by the IT Panel (available here).

Questions for software suppliers

The questions which you may wish to ask your software suppliers are as follows:

Location of servers storing data relating to professional work

1. Do you store data (including any backup data) on servers located outside chambers? If Yes - continue to Q2. If No, continue to Q6.

2. What type of data do you store on servers located outside chambers (including backup data)?

3. Where are the servers located on which data is stored?

4. Do you store backup data on servers located elsewhere (including cloud services)? If so, where are those servers located?

5. Is the data encrypted? Who holds the key/credentials and how securely are they stored?

6. Do you have the ability to gain access directly into the chamber's server or network without specific intervention, knowledge or authority of a representative of Chambers on each occasion?

7. What is your procedure for ensuring the data security of files transferred from chambers to you when resolving faults or upgrading systems?

8. Do you make use of third party services? If so, do you rely on servers/services outside your direct physical control to which client data is transferred?

Security

9. Which elements of continuity or backup in a system provided to chambers relies on the synchronisation and/or storage of data both in chambers and/or in the cloud?

10. Are credentials, including administrative or support remote access credentials, used to access a system in chambers, unique to each set of chambers?

11. Are you enforcing an adequate password strength and renewal regime?

12. Do you have systems which store credentials to access confidential systems in chambers, and if so, are those details encrypted?

13. When specific examples of system faults are made which could involve a support firm identifying individual clients of chambers, how does the fault diagnosis, escalation and resolution process mitigate these risks (e.g. reporting a fault to the Practice Management System provider)?

Connection with US companies

14. Where were you incorporated?

15. Where is your principal place of business?

16. Do you have a parent company which was incorporated or has a principal place of business outside the EU? If so, please give details.

17. For each server on which you store data (including backup data) please answer the following questions:

    17.1. Who owns the server?

    17.2. Where was the company which owns the server incorporated?

    17.3. Where is the principal place of business of the company which owns the server?

    17.4. Does the company which owns the server have a parent company which was incorporated or has a principal place of business outside the United Kingdom? If so, please give details.

Policy

18. What is your policy about compliance with Data Protection Act 2018 and the GDPR if you receive a request for disclosure from US authorities?

19. What procedure do you follow in informing customers if access to their data is requested or demanded by others?

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of information security**. It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it.** It does not comprise - and cannot be relied on as giving - legal advice. It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please refer to the professional practice and ethics section of the Bar Council's website here.