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 on servers located in the US or by US-owned companies on servers located anywhere
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 2025
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 United States (US) authorities without your knowledge when keeping that information on servers which are situated in the US or servers situated anywhere but 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 and other US laws confer power on certain US authorities to access data stored on facilities which use servers situated in the US and/or which are provided by US persons or companies, without the knowledge or 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 sought to provide a legal mechanism for the recovery by US authorities of personal data stored anywhere in the world by US-based Internet Service Providers (ISP) 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 were criticised by many observers, including the Council of Bars and Law Societies of Europe (CCBE), as being inadequate.

6. Data transfers between the European Union (EU) (and United Kingdom (UK)) and the US were sought to be facilitated by the EU/US Privacy Shield, which, however, was invalidated by the European Court of Justice (ECJ) in its decision of 16 July 2020 in the Schrems II case (Case C-311/18). One of the factors leading to that invalidation was the inadequacy of the US Cloud Act safeguards. Although alternative mechanisms such as Standard Contractual Clauses were and continue to be available to facilitate data transfers to the US, this does not remove the risks of surveillance posed by the US Cloud Act.

7. In light of the concerns expressed following the Schrems 2 decision, President Biden issued an Executive Order dated 7 October 2022 introducing further safeguards under the Cloud Act for data transfers to the US, in light of which the European Commission promulgated a new EU-US Data Privacy Framework in 2023. The UK Government promulgated the UK Extension to the EU-US Data Privacy Framework (UK Extension) under Article 45 of the UKGDPR, which came into force on 12 October 2023. A guidance note can be found at:

https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-factsheet-for-uk-organisations.

8. Notwithstanding the UK Data Privacy Framework, there exist real practical problems with regard to protection of data subject to Legal Professional Privilege (LPP), as discussed below. Furthermore, under the US Cloud Act, not only is data stored in the US susceptible to the provisions of the Act, but so, too are cloud providers who are "US persons". This covers not only Companies based in the US, but also US companies with subsidiaries in the UK. Such companies would be obliged to comply with the provisions of the Act.

9. 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 without being a subsidiary as such. 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.

10. Where 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 UK 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 UK GDPR regime which has a bearing on the duties of barristers as data controllers and chambers as data controllers.

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

12. Data held by an ISP on behalf of a barrister or chambers is likely in most instances to be protected by Legal Professional Privilege (LPP). Research by the CCBE suggests that many ISPs are unable to identify such data, or in a position even to be able to assert LPP on behalf of the data controller. Furthermore, LPP may not be available as a defence to a request to hand over data made under the US Cloud Act and other US surveillance provisions.

Your obligations

13. Data controllers are obliged under the UK 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.

14. 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 be waived only by the client or as is required or permitted by law.

Advice to data controllers and barristers

15. 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)

16. 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 and UK and which does not have adequate data protection laws.

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

18. 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 Cloud Act and other relevant US laws.

19. 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.

20. 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.

21. You should review the:

- ICO guidance on data protection impact assessments
- ICO guidance on cloud computing
- Advice on cloud computing provided by the Bar Council's IT Panel

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

- Do you store data (including any backup data) on servers located outside chambers? If Yes - continue to Q2. If No, continue to Q6.
- What type of data do you store on servers located outside chambers (including backup data)?
- Where are the servers located and which data are stored?
- Do you store backup data on servers located elsewhere (including cloud services)? If so, where are those servers located?
- Is the data encrypted? Who holds the key/credentials and how securely are they stored?
- 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?
- What is your procedure for ensuring the data security of files transferred from chambers to you when resolving faults or upgrading systems?
- 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?
- Do you have a means of identifying data stored on your server which are subject to LPP?
- If requested or ordered by a competent authority to disclose such data, do you have a policy of asserting LPP and declining to accede to the request, at any rate, without reference to the data controller?

Security

- 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?
- Are credentials, including administrative or support remote access credentials, used to access a system in chambers, unique to each set of chambers?
- Are you enforcing an adequate password strength and renewal regime?
- Do you have systems which store credentials to access confidential systems in chambers, and if so, are those details encrypted?
- 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

- Where were you incorporated?
- Where is your principal place of business?
- Do you have a parent company which was incorporated or has a principal place of business outside the EU or UK? If so, please give details.
- For each server on which you store data (including backup data) please answer the following questions:

    1. Who owns the server?
    2. Where was the company which owns the server incorporated?
    3. Where is the principal place of business of the company which owns the server?
    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

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

- What is your policy about compliance with a request for disclosure from US authorities where the request relates to material which is or may be protected by LPP?
- What procedure do you follow in informing customers if access to their data is requested or demanded by others?

Important Notice

This document and sample policy has been prepared by the Bar Council to assist barristers and chambers 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. Read more information about the status and effect of this document on the Bar Council Ethics and Practice Hub.