The Bar Council

What to do if you lose papers, or if your data security is breached

Purpose:	To guide all barristers on good practice and legal obligations following a personal data breach or loss of papers
Scope of application:	All practising barristers
Issued by:	The Information Technology Panel
Originally issued:	January 2017
Last reviewed:	February 2024
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.**

1. You must take proper care of information belonging to your client and others.

2. rC15 of the BSB Handbook (version 4.7, in force 20 September 2023) requires barristers to protect the confidentiality of a clients' affairs:

> *"… you must protect the confidentiality of each client's affairs, except for such disclosures as are required by law or to which your client gives informed consent".*

3. From 25 May 2018 barristers have been obliged to comply with the General Data Protection Regulation ("GDPR"),[1] and after Brexit the UK GDPR,[2] in relation to the personal data of clients and other individuals. Self-employed barristers are GDPR data controllers of their clients' (and likely others') personal data.

4. GDPR Art. 5(1) requires data controllers to process personal data (which includes both electronic data and paper files) using appropriate security, so that it is

[1] See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[2] See: https://www.legislation.gov.uk/uksi/2019/419, references to GDPR in this document should be read as to referring to the UK GDPR.

protected against accidental loss, destruction or damage. Art. 32 requires the implementation, testing and regular evaluation of appropriate security measures, as follows:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> (d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

5. It is therefore the individual responsibility of each self-employed barrister to take appropriate precautions in relation to the security of the equipment and communications channels that they use, or that are used on their behalf.

6. If you lose a client's papers, or suffer a breach of security which affects someone's data (whether or not it is your client's data), you may be in breach of these various obligations. This might happen in many different ways. For example:

a) by leaving papers on a train

b) if your laptop, tablet or smartphone is stolen

c) if your computer or mobile device becomes infected by a virus or other malware, perhaps as a result of opening an attachment to an email or clicking on a link in a phishing email.

7. GDPR Art. 4(12) defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Other GDPR articles require you to keep written records of any personal data breaches, and in some circumstances to notify them to the Information Commissioner's Office (ICO) and to the individuals whose data is affected.

8. General guidance on how to prepare in advance for a personal data breach, and what to do if one occurs, is provided on the ICO's website,[3] and you should familiarise yourself with it.

9. The ICO may impose a penalty of up to €20 million or 4% of global turnover on a controller or a processor following a personal data breach. GDPR Art. 83 says that when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given inter alia to the following:

> (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
>
> (b) the intentional or negligent character of the infringement;
>
> (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
>
> (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
>
> (f) any relevant previous infringements by the controller or processor;
>
> (g) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
>
> (h) the categories of personal data affected by the infringement.

The ICO may also require undertakings as to your future conduct, for example an undertaking to encrypt a laptop computer and to keep it under lock and key when not in use.

10. As mentioned above, GDPR Arts. 33 and 34 require records of personal data breaches to be kept, and that certain breaches be notified to the ICO and to the individuals whose data is affected:

a. Keeping records and notifying the ICO (GDPR Article 33):

i. *In the case of a personal data breach, a data controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the [ICO], unless the personal data breach is unlikely to result in a risk to the rights and*

[3] See: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

ii. *A data processor must notify the controller without undue delay after becoming aware of a personal data breach. This means that, for example, clerks should inform barristers of a breach of Chambers' security as soon as possible, as they are processing information for the data controller barristers.*

iii. *The notification referred to in (i) above shall at least:*

(1) *describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*

(2) *communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*

(3) *describe the likely consequences of the personal data breach;*

(4) *describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

iv. *Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*

v. *The data controller must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the [ICO] to verify compliance with the GDPR.*

b. Notifying data subjects (GDPR Article 34):

i. *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller must communicate the personal data breach to the data subject without undue delay.*

ii. *The communication to the data subject must describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (ii), (iii) and (iv) above.*

iii. *The communication to the data subject will not be required if any of the following conditions are met:*

(1) *the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*

(2) *the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in (i) is no longer likely to materialise;*

(3) *it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.*

iv. *If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in (iii) above are met.*

11. If a breach of confidentiality or a failure to keep information secure amounts to "serious misconduct", a barrister could be obliged to report him or herself or another barrister to the Bar Standards Board ("BSB") under rules rC65.7 or rC66 of the Code of Conduct. There is also an obligation to take all reasonable steps to mitigate the effects, according to the guidance (gC94) under rule rC65.

12. If you report a data breach to the ICO and they take disciplinary action against you, you will need to report this to the BSB under rC65.3. If the ICO takes no action, there is no obligation under rC65.3 for you to report to the BSB. However, you should also consider whether your conduct posed a "serious risk to the public" under gC96.10 which consequently would trigger your duty to report yourself to the BSB under the serious misconduct provision of rC65.7. Self-reporting to the BSB must be done promptly.

13. You and/or your Chambers should have a Data Breach Response Plan, and this should be followed. A draft Data Breach Response Plan, which may be adapted for your or your Chambers' use, is available here.

Breach management

Containment and recovery

14. Unless you are sure that the breach will not result in a risk to data subjects, the first step will be to inform the appropriate person in Chambers of the breach, in accordance with your Chambers Data Breach Response Plan.

15. If the breach relates to your IT facilities, it will usually be necessary to take advice from an IT consultant on the steps to be taken to limit the damage caused and to prevent further damage or a repetition.

Assessing the risks

16. It is important to consider the risks arising from the loss. There could be a big difference between the loss of one ring binder of papers and the loss of an unencrypted laptop. The assessment needs to consider the potential adverse consequences for clients, whether they are companies or individuals, and for individuals who are not clients (e.g. names and contact details in a database of a company's customers). The questions to consider include the following:

a) What type of data is involved (for example, banking details, criminal records, health records)?

b) How sensitive is the data? Some data, such as that in health records, is sensitive because of its very personal nature, while other data, such as bank account details, is sensitive because of what might happen if it is misused. In particular, is the data 'Special Category personal data' within GDPR Art. 9, which is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health and data concerning a natural person's sex life or sexual orientation. Is it personal data relating to criminal convictions and offences or related security measures, within Art. 10?

c) If a device has been lost or stolen, are there any protections in place for the data, such as encryption?

d) What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.

e) Regardless of what has happened to the data, what could the information tell a third party about the individual? Is there a risk of identity theft? Some data, even if it is "Special Category" data (e.g. trade union membership) could mean very little to an opportunistic laptop thief, while the loss of apparently trivial snippets of information (e.g. name, address, telephone number, National Insurance number) could help a determined fraudster to build up a detailed picture of other people to exploit.

f) How many individuals are affected by the breach? It is not always the case that the bigger risks will accrue from the loss of large amounts of data, but this is certainly an important determining factor in the overall risk assessment.

g) Who are the individuals whose data has been breached? Whether they are lay or professional clients or witnesses, for example, may affect the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks.

h) How will the loss of data affect the individuals concerned? What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and impacts on other aspects of their life?

i) Are there wider consequences to consider such as a risk to public health or loss of public confidence?

j) If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Notification of breaches

17. Informing Chambers and, in the event of serious misconduct, the BSB, has already been referred to above.

18. The requirement in GDPR Arts. 33 and 34 to inform the ICO and data subjects in specified circumstances has also been set out above. Failure to notify the ICO may be regarded as an aggravating factor when the ICO is considering whether to impose a fine. The notification to the ICO must usually be made within 72 hours. This deadline may be very short, especially if the breach occurs on a Friday evening or a Saturday and investigations are required in order to work out whether data has been compromised.

19. The ICO has provided a self-assessment tool to help you work out whether you need to report a breach to them. Breaches may be reported to the ICO by telephone,

or using a downloadable form.[4] You will have to provide (amongst other things) your details, information about the incident, the information at risk and remedial actions taken.

20. Where appropriate, the police, insurers and/or indemnity providers such as BMIF, should also be informed.

21. Where there is a significant risk of substantial damage to a client, you need to consider whether to inform your solicitors, your lay client, or opposing parties, especially where sensitive data is concerned. Reporting to the professional client is mandatory when instructed by the Government, and may also be required by contract terms. The Bar Council's document on Information Security states that when a loss or theft of Confidential Material occurs, Chambers, the professional client and (if appropriate) the police should be immediately informed.

Evaluation and response

22. After investigating the causes of the breach and taking steps to limit the damage caused, it is important to review your procedures, methods of working and configuration of IT systems and equipment to see whether they need to be improved in order to prevent a repetition. If you are reading this guidance before there has been a breach, then considering these issues may prevent a breach occurring. The following points will assist you with such a review:

a. Make sure you know what data you have and where and how it is stored. Dealing with a data security breach is much easier if you know which data is involved.

b. Think about whether there are categories of data which you do not need to retain, and delete unnecessary data.

c. Think about whether your data is being stored in places where it may not be sufficiently secure, for example on Gmail or Dropbox, and take steps to store it more securely.

d. Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks.

e. Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.

[4] Details are at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

f. Adopt a Data Breach Response Plan for dealing with data security breaches, and identifying a group of people responsible for reacting to reported breaches. See the draft Data Breach Response Plan, which is available here.

Important Notice

This document and its annexed sample incident response plan has been prepared by the Bar Council to assist barristers on matters of IT. **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 see here.