BAR STANDARDS BOARD

REGULATING BARRISTERS

Data Sharing Protocol for the sharing and disclosure of information between

The Bar Standards Board

And

The Council of the Inns of Court

And

The Honourable Society of The Inner Temple

And

The Honourable Society of The Middle Temple

And

The Honourable Society of Gray's Inn

And

The Honourable Society of Lincoln's Inn

Contents

We can provide our literature in different formats. If you require this information in a different format, please contact us on contactus@barstandardsboard.org.uk or 020 7611 1444.

Purpose

1. This document ('the Protocol') provides a framework for the collection, sharing, retention and destruction of information between the independent data controllers; the Bar Standards Board (BSB), the Council of the Inns of Court (COIC) and each of the four Inns of Court: Inner Temple, Middle Temple, Gray's Inn and Lincoln's Inn. This is to support the BSB in the administration of its regulatory functions and to provide quality assurance to obligations administered by the Inns of Court and COIC are done so effectively.

2. The Protocol should be read in conjunction with the Memorandum of Understanding (MoU) between COIC, the four Inns and the BSB which sets out the responsibilities of the Parties relating to the education and training for the Bar, and any statutory, regulatory or other policies and statements which apply[1].

Background

3. In accordance with the guidance from the Information Commissioner's Office (ICO) and the BSB's Information Security Policy, we set out below the background for the introduction of this Protocol.

4. The sharing of personal data set out in this Protocol is necessary to ensure that the BSB has adequate regulatory oversight of students, barristers and the responsibilities of COIC and the Inns, as set out in the MOU. The sharing and use of the personal data is, therefore, necessary for the performance of a task carried out in the public interest and in the exercise of the BSB's authority under the Legal Services Act 2007. The Parties may also share special category data, as it relates to the individual's health[2] and criminal records information, as the Legal Services Act 2007 requires the BSB to protect and promote the public interest (e.g. protecting the trust and confidence the public places in the profession that only those who are fit and proper are Called to the Bar).

5. The risks of transferring shared personal data include a risk of security breaches. However, this is mitigated by the robust security policies and measures which each Party has in place. There is also a risk that we do not use the shared personal data in line with the GDPR requirements. This risk is mitigated by the Parties upholding this Protocol and their obligations within the MOU.

6. The Parties agree that the shared personal data set out in Annex 1 is the least amount of personal data required to be shared to ensure the BSB is assured that their regulatory functions are administered satisfactorily. This also sets out the purpose for which the personal data is shared between the Parties.

[1] The Privacy Statement which applies to the BSB can be accessed here: https://www.barstandardsboard.org.uk/footer-items/privacy-statement/

[2] For example, this may be shared as part of the ICC hearings, following a disclosure by an applicant in the admissions declaration.

7. Annex 2 sets out the individuals who are the nominated Data Protection Officers/Leads (DPO) and therefore have responsibility to ensure that only those who require access to the shared personal data are able to do so.

Definitions

Bar Standards Board – means the independent regulatory body of the General Council of the Bar of England and Wales

Data controller - means a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any shared personal data is processed[3].

Data processor in relation to shared personal data - means any person (other than an employee of the data controller) who processes the shared personal data on behalf of the data controller[4].

Data Protection Officer/Lead – referred to as DPO throughout the document means the nominated individual within each Party who oversees the Party's processing of shared personal data and ensures it is complying with its data protection obligations under the Data Protection Legislation, including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

COIC – means the Council of the Inns of Court and includes the Inns Conduct Committee and the Bar Tribunals and Adjudication Service.

Inns of Court – means each of the four Inns of Court; the Honourable Society of The Inner Temple, the Honourable Society of The Middle Temple, the Honourable Society of Gray's Inn and the Honourable Society of Lincoln's Inn.

Memorandum of Understanding – means the document agreed between the BSB, COIC and the four Inns of Court in relation to education and training for the Bar.

Party – means one of the BSB, COIC, or the Inns

Parties – means more than one Party

Permitted Recipients - The parties to this agreement, the employees of each party, any third parties engaged to perform obligations in connection with this agreement.

Personal Data Breach – has the meaning set out in the Data Protection Legislation

Processing - means any operation or set of operations which is performed on shared personal data or on sets of shared personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Shared Personal Data - The personal data to be shared between the parties under Annex 1 of this agreement. 'Personal data to be shared' will be construed accordingly.

Information governance

[3] In accordance with the Data Protection Legislation, including the Data Protection Act 2018 and General Data Protection Regulation
[4] Ibid

8. Each party shall comply with all the obligations imposed on a controller under the Data Protection Legislation.

9. Where there is a need to make a public statement about the exchange of information, e.g. as a result of a press enquiry, the Parties may liaise with each other before finalising the individual statements each Party will make.

10. The Parties agree to the following responsibilities. This has been specified in more detail in Annex 1:

    a) Data controller – Each Party; the BSB, COIC and the Inns of Court are independent data controllers.

    b) DPO – Representative individual/s within each Party who is accountable for:

        i. ensuring that they understand the types of information received, generated, stored and transferred for their area of work; and

        ii. ensuring the shared personal data and information is managed in accordance with this policy and any other relevant policies and statutory requirements relevant to each Party.

11. The Parties agree that their DPOs will at all times comply with the DPA & GDPR complying with the above obligations, the DPO for each Party will have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Information sharing

12. Each party acknowledges that one party (the Data Discloser) will regularly disclose to the other party (the Data Recipient) shared personal data collected by the Data Discloser for the purposes for which it is shared.

13. The Parties agree that where personal data is shared and disclosed its use is restricted to regulatory purposes unless onward disclosure to other agencies is necessary in the public interest and is lawful.

14. The Parties have a requirement under the Data Protection Legislation including the DPA and GDPR to provide data subjects with a Privacy Notice. All Parties agree to include details of this Data Sharing Protocol within their respective Privacy Notices.

15. The Parties agree to identify points of contact in their respective organisations to facilitate the sharing and disclosure of information. This is set out in Annex 2.

16. The Parties will exchange information to the extent permitted by law, and in a timely fashion, to enable each other to process it according to their own internal procedures. The Parties will disclose the shared personal data with other organisations in accordance with their respective privacy policies.

The personal data to be shared

17. Each party shall:

a) ensure that it has all necessary notices and consents in place to enable lawful transfer of the shared personal data to the permitted recipients for the purpose for which it is shared; and

b) give full information to any data subject whose shared personal data may be processed under this agreement of the nature of such processing. This includes giving notice that, on the termination of this agreement, shared personal data relating to them may be retained by or, as the case may be, transferred to one or more of the Permitted Recipients, their successors and assignees as relevant; and

c) use any templates specified by another Party, where practicable, for the sending of shared personal data.

18. The Parties shall not transfer any shared personal data received from the Data Discloser outside the EEA unless the transferor:

a) complies with the provisions of Articles 26 of the GDPR (in the event the third party is a joint controller); and

b) ensures that (i) the transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 GDPR; or (iii) one of the derogations for specific situations in Article 49 GDPR applies to the transfer.

19. The shared personal data collected and stored by each Party is set out in Annex 1 and should be used for the stated purposes only, and in accordance with relevant statutory, regulatory and policy provisions.

20. The Parties agree to inform individuals who provide their data which is shared under this Protocol of the existence of this protocol. The BSB will do this through a Privacy Notice and COIC and the Inns through their Privacy Notices and Data Protection Policies.

Retention of shared personal data

21. In accordance with statutory requirements, the Parties shall only retain shared personal data for as long as is necessary for the legitimate purposes for which the shared personal data is processed (which may be different for each party), unless the retention of the shared personal data is required for archiving purposes which are in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) of the GDPR or other applicable provisions under the Data Protection Legislation. This period is determined by the DPO within each Party.

22. Each Party should ensure that when those legitimate purposes come to an end, the Parties shall securely delete the shared personal data.

23. The Parties agree to regularly review the shared personal data held to ensure adherence to this policy and to ensure it is kept up to date and accurate.

Destruction and disposal of shared personal data

24. The Parties are responsible for ensuring that shared personal data is destroyed securely, having regard to the relevant statutory and regulatory requirements and the timeframes set out in this Protocol.

25. Under no circumstances should paper documents containing shared personal data be placed into general refuse as to do so risks the unauthorised disclosure of such information to third parties. Such disclosure would be a breach of the Data Protection legislation.

26. Paper documents must be destroyed on site (e.g. by shredding) or placed in the specially marked “Restricted Waste”, or similar, containers/bags within the Parties’ buildings.

27. The Parties will ensure that electronic documents are deleted to the extent that they are virtually impossible to retrieve. In the case of electronic systems such as Case Management Systems, only individuals with the necessary authority will be able to delete information to the required extent.

28. Set out below are the key considerations for the retention and disposal of shared personal data:

    a) the nature of the shared personal data (paper or electronic) and which sections of the shared personal data will be destroyed;

    b) whether the shared personal data must be retained to fulfil any statutory and/or regulatory requirements;

    c) whether the shared personal data should be retained in case of a dispute; and

    d) whether the shared personal data should be retained to meet the operational needs of the Parties and if so, whether this can be achieved by redacting the personal information; and

    e) whether the risks of retaining or destroying the information have been properly assessed.

Data security

29. The Parties will ensure that they have in place appropriate technical and organisational measures, to protect against unauthorised or unlawful processing of shared personal data and against accidental loss or destruction of, or damage to, shared personal data. This includes, but is not limited to, the below measures:

    a) In accordance with section 32(1) of the GDPR, 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 Parties will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate:

        i. the encryption of shared personal data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. password protecting documents;

iv. the ability to restore the availability and access to shared personal data in a timely manner in the event of a physical or technical incident;

v. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Procedures for dealing with access requests, queries and complaints

30. Individuals should submit a subject access request to each organisation they are seeking their shared personal data from. Each Party shall provide contact details for their DPO to support liaison between the Parties, should this be required and permissible, as set out in Annex 2. The DPO shall also be the first point of Call to whom any queries and complaints should be sent.

31. The Parties' obligations to comply with the above rights are subject to certain exemptions in the Data Protection Legislation.

32. The data subject also has the right to complain to the ICO if they are not satisfied with the way the Parties use their information. The data subject can contact the ICO by writing to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Review

33. The Parties agree that the Protocol will be effective by 1 September 2020.

34. The Parties will monitor the operation of the Protocol and formally review it every year. Meetings to discuss any issues arising will be held as necessary to monitor its effectiveness.

35. The purpose of these meetings is to:

a) provide feedback on the quality of the sharing and disclosure of information;

b) review the effectiveness of processes in place to support the sharing and disclosure of information;

c) discuss issues of wider concern that may impact on how the Parties operate together;

d) alert each other to and discuss emerging trends, issues, risks or other activities that may be of interest; and

e) discuss any other issues of concern to either of the Parties.

Resolution of conflicts

36. The Parties will cooperate with each other if a dispute arises under this Protocol. Parties will seek to:

    a) avoid disputes arising in the first instance; and

    b) settle disputes amicably if/when they do arise.

37. Where disputes do arise, the points at issue need to be fully documented in a format readily understood by a third party. Where necessary, disputes will be referred to the senior management in the respective Party for resolution.

38. Any problems or concerns in an individual case of information sharing should be channelled via the designated individuals, in Annex 2, who will seek to resolve the matters. In the event that the issues cannot be resolved, the matters will be escalated via the relevant line management chain of each Party.

Personal data breaches

39. Any actual or suspected Personal Data Breach (of shared personal data) must be reported to the relevant DPOs (for the Party where the breach occurred and the Party(ies) who supplied the information) immediately upon becoming aware of such breach, so that the Parties can comply with their accountability obligations under the DPA and GDPR. They will be responsible for ensuring that the protocols in place within their own organisation will be adhered to.

40. Those individuals within the Parties who will have access to the shared personal data set out in Annex 1 will receive adequate training to enable them to recognise when there may be a Personal Data Breach (of shared personal data) and know how to escalate the incident to the appropriate person, or team, within their Party to determine whether a breach has occurred.

41. Each Party agrees to prepare an action plan for addressing any Personal Data Breaches (of shared personal data) that occur within their organisation, including having a process to assess the likely risk to individuals as a result of a breach. This should be done on a case by case basis.

42. Each Party will allocate responsibility for managing Personal Data Breaches (of shared personal data) to a dedicated person or team within their organisation who will be aware of:

    a) The relevant supervisory authority for the processing activities which the Parties undertake;

    b) The process to notify the ICO, if necessary, and the other Parties of a breach within 72 hours of becoming aware of it, even if all the details are not known;

    c) What information must be provided to the ICO as a result of a breach, if the breach meets the criteria for being reported;

    d) The process to inform affected individuals about a breach and what information about the breach must be provided to them, if the breach meets the criteria for being reported; and

e) The requirement to document all breaches, even if they don't need to be reported[5].

43. The Parties agree to review the Protocol in light of the breach. Any significant changes required as a result of the breach should be publicised.

Indemnity

44. Each party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the breach of the Data Protection Legislation by the indemnifying party, its employees or agents, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it.

Failing to comply with the data sharing protocol

45. Following notification of a breach of the Data Protection Legislation by a party to this protocol, and reporting to the ICO, where appropriate, the Parties may review the breach together and recommend remedial actions to avoid such breaches in the future.

Publication

46. The Protocol is a public document and the Parties may publish it as they see fit.

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

Annex 1 – the personal data to be shared

It is noted that contact details are subject to change and therefore the Parties shall provide this data on a best endeavours basis at the point specified in this Annex.

	Personal data to be shared by the Inns to the BSB before Call			
	The information to be collected	**How it will be collected**	**What it will be used for**	**When will it be shared**
	Admission to an Inn			
1	When a lawyer is seeking to transfer or be readmitted to the Bar: 1. MyBar number (if available); 2. Name 3. Date of birth 4. The Inn they are admitted to	Spreadsheet	Used by the BSB to check our records so we can share any matters which may question whether they are a fit and proper person	Within 10 working days of the application
	Fit and proper person checks on admission to an Inn and, or prior to Call			
2	For hearings at the ICC: 1. MyBar number (if available); 2. Name; 3. Date of birth 4. The category of conduct; 5. Detail of the conduct[6] 6. The outcome of the hearing	Spreadsheet	Used by the BSB to determine whether to appeal an ICC hearing to the High Court.	Within 14 working days of the outcome of the ICC hearing.

[6] This may include the length of time over which the conduct occurred, special category data and criminal convictions

3	In accordance with the assurance process, the BSB may request a sample of any fit and proper person decisions and require: 1. MyBar number (if available); 2. Name; 3. Date of birth; 4. The category of conduct; 5. Detail of the conduct[7]; and 6. The outcome of the hearing.	Spreadsheet	Review by the BSB to satisfy itself that fit and proper person checks are being conducted correctly against the relevant Guidelines to promote consistency in decision making and identify improvements.	Within 14 days of a BSB request as part of their assurance (as set out in schedule 4 of the MOU).
	At Call			
4	1. MyBar number (if available); 2. Name; 3. Date of birth; 4. Date of admission; 5. Inn admitted to; 6. Date of Call; 7. Email address; and 8. Contact number. In accordance with Schedule 2 of the MOU, the BSB reserves the right to review a student's record to satisfy itself that the requirements of qualifying sessions have been complied with. This will not contain any additional personal data to the above.	Spreadsheet	Included on the individual's record so the BSB knows the Inn they are a member of and when they have been Called.	Within 7 working days of Call

[7] This may include the length of time over which the conduct occurred, special category data and criminal convictions.

	Personal data to be shared by the Inns to the BSB after Call			
	The information to be collected	**How it will be collected**	**What it will be used for**	**When will it be shared**
5	Barristers seeking voluntary disbarment 1. MyBar Number (if available); 2. Name; and 3. Date of birth.	By email	The BSB to check whether we have details of ongoing conduct investigations and to provide this to the Inns	Within 7 working days of being notified that the barrister wishes to voluntarily disbar
6	Name change details 1. MyBar Number (if available); 2. Name; and 3. Date of birth.	By email	To ensure the practising data if up to date	Within 7 working days of notification to the Inn's and provision of name change documentation

	Personal data to be shared by the BSB to the Inns before Call			
	The information to be collected	**How it will be collected**	**What it will be used for**	**When will it be shared**
7	For transferring lawyers and those seeking readmission: 1. Name; 2. Date of birth; 3. Any factual information which may question whether they are a fit and proper person,	Email	The Inns/ICC can use the information at the hearing	Within 7 working days of the request

	following a request from the Inn as set out in line 1[8] . This may include: • The original finding that led to the disbarment • Withdrawn or dismissed cases[9] • Certificates of good standing • Disciplinary action by another regulator • Concerns over fraudulent certificates			
8	Enrolment spreadsheet showing the number of students enrolled at each Inn, subdivided by: • Student name; • MyBar number if available • Date of birth; • AETO (Provider/Site) • The Inn the student is a member of	Spreadsheet	So that the Inns hold the details of a student's vocational provider and to facilitate the administration of Fit and Proper Person Checks and Qualifying Session Programmes	Within 7 working days of the BSB receiving this personal data from the provider.
9	Bar Transfer Test (BTT) pass list • Name • Email address • Home address • Date they passed the BTT	Spreadsheet	So that the Inns are able to admit and Call students	Within 7 days of the BSB receiving the pass list.

	Personal data to be shared by the BSB to the Inns after Call			
	The information to be collected	**How it will be collected**	**What it will be used for**	**When will it be shared**

[8] This may include special category data or criminal convictions

[9] These matters may have been withdrawn or dismissed because they relate to the same barrister who was disbarred but it was decided not to pursue an investigation or hearing, in addition to the disbarment matter

10	Details of any ongoing conduct investigations for individuals who are seeking voluntary disbarment	By email	The Inns will use the shared personal data to consider whether the individual should be allowed to voluntarily disbar or whether this should be postponed until the outcome of any investigations	Within 7 days of being notified that the barrister wishes to voluntarily disbar

Annex 2 - Data Protection Officer/Lead

Figure 1 – Data Protection Officer/Lead at the BSB - This table sets out the contacts at the BSB through which contact between the Parties will be channelled.		
Data Protection Officer/Lead	The shared personal data below is that which the DPO is responsible for responding to data access requests, queries or complaints.	The shared personal data below is that which the DPO is responsible for determining the individuals within their team who can access the shared personal data.
Head of Training Supervision & Examinations	• Student Membership information	• Student Membership information
Head of Authorisation Head of Supervision	<u>Authorisations</u> • Applications to Inns by pupil supervisors • Misconduct matters for transferring lawyers	<u>Authorisations</u> • Applications to Inns by pupil supervisors • Misconduct matters for transferring lawyers <u>Supervision</u> • Student conduct
Records manager		• Membership information
Head of Investigations and Hearings	• Student conduct • Individuals seeking voluntary disbarment • Conduct matters for voluntary disbarment • Applications to Inns by pupil supervisors	• Student conduct • Individuals seeking voluntary disbarment • Conduct matters for voluntary disbarment • Applications to Inns by pupil supervisors
Head of Research and Information[10]		• All of the above

Figure 2 – Data Protection Officer/Lead at COIC - This table sets out the contacts at the BSB through which contact between the Parties will be channelled.

[10] The Head of Research and Information will be responsible for determining the individuals within their team who will need access to the data which will be shared by COIC and the Inns to provide reports as required. However, as they are not the Data and Information Owners of the data, as this is held by the other individuals identified within Figure 1, they will not be responsible for channelling the contact between the Parties or responding to data access requests, queries or complaints in the first instance. This will be directed to the other individuals listed above, who may delegate as they consider necessary.

Position held	DPO are the designated contacts for the different sets of shared personal data and for responding to data access requests, queries or complaints.	DPO responsible for determining the individuals within their team who can access the sets of shared personal data.
Director of Operations	**All**	**All**

Figure 3 – Data Protection Officer/Lead at The Inner Temple - This table sets out the contacts at the Inner Temple through which contact between the Parties will be channelled.		
Position held	DPO are the designated contacts for the different sets of shared personal data and for responding to data access requests, queries or complaints.	DPO responsible for determining the individuals within their team who can access the sets of shared personal data.
Membership Registrar	**All**	**All**

Figure 4 – Data Protection Officer/Lead at The Middle Temple - This table sets out the contacts at the Middle Temple through which contact between the Parties will be channelled.		
Position held	DPO are the designated contacts for the different sets of shared personal data and for responding to data access requests, queries or complaints.	DPO responsible for determining the individuals within their team who can access the sets of shared personal data.
Director of Corporate Services	**All**	**All**

Figure 5 – Data Protection Officer/Lead at Gray's Inn - This table sets out the contacts at Gray's Inn through which contact between the Parties will be channelled.		
Position held	DPO are the designated contacts for the different sets of shared personal data and for responding to data access requests, queries or complaints.	DPO responsible for determining the individuals within their team who can access the sets of shared personal data.
Director of Finance	**All**	**All**

Figure 2 – Data Protection Officer/Lead at Lincoln's Inn - This table sets out the contacts at Lincoln's Inn through which contact between the Parties will be channelled.		
Position held	DPOs are the designated contacts for the different sets of shared personal data and for responding to data access requests, queries or complaints.	DPOs responsible for determining the individuals within their team who can access the sets of shared personal data.
Assistant Under Treasurer	**All**	**All**