



The Bar Tribunals & Adjudication Service

The Council of the Inns of Court

Information Security Policy

Contents

1. Introduction	2
2. Our policy commitment	2
3. The General Data Protection Regulation	2
4. Duties	4
5. Disclosure and transfer of personal data	5
6. Destruction of personal data	5
7. Data subject's access requests.....	6
8. Data Retention, Storage & Disposal.....	6
9. Review	6

Date of implementation: *March 2013*
Date of last review: *February 2019*
Date of next review: *February 2020*

The Bar Tribunals & Adjudication Service

9 Gray's Inn Square,
London
WC1R 5JD
T: 020 3432 7350
E: info@tbtas.org.uk

The Council of the Inns of Court. Limited by Guarantee
Company Number: 8804708
Charity Number: 1155640
Registered Office:
9 Gray's Inn Square, London WC1R 5JD

1. Introduction

- 1.1 The Bar Tribunals and Adjudication Service ('BTAS') is responsible for recruiting; appointing, administering and adjudicating Disciplinary Tribunals, including Tribunals which consider the most serious allegations of professional misconduct against barristers.
- 1.2 In addition to Disciplinary Tribunals, BTAS has similar responsibilities for Fitness to Practise hearings and Interim Suspension Panels for barristers.
- 1.3 BTAS also administers and supports the Inns' Conduct Committee (ICC), a committee responsible for adjudicating on any misconduct issues arising from applications for admission to an Inn of Court or misconduct matters relating to student members of an Inn.
- 1.4 To fulfil its responsibilities to recruit staff and appoint individuals to sit on disciplinary panels and conduct committees, BTAS will collect process and store personal information.
- 1.5 COIC is a registered data controller with the Information Commissioner's Office.
Registration: Z3206735.

2. Our policy commitment

- 2.1 BTAS is committed to the protection of personal information or data; in particular BTAS is committed to the principles set out in the General Data Protection Regulation ('GDPR').
- 2.2 The purpose of this policy is to;
 - i. Outline BTAS's commitment to the lawful handling of personal information and data;
 - ii. Acquaint those handling personal data with the principles set out in the GDPR; and,
 - iii. Outline the duties emanating from the GDPR.

3. The General Data Protection Regulation

- 3.1 The Regulation has two key purposes:
 - i. To regulate the use by those who obtain, control and process personal data of living individuals.

- ii. To provide certain rights (such as accessing personal information) to those living individuals (known as data subjects) whose data is held.

3.2 The Regulation has six key principles, that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.3 The Regulation provides conditions for the processing of any personal data. It also makes a distinction between personal data, 'special category' personal data and criminal offence data and requires the latter two to be handled especially carefully.

3.4 Personal data includes information relating to natural persons who:

- a) can be identified or who are identifiable, directly from the information in question; or

- b) who can be indirectly identified from that information in combination with other information.
- 3.5 Special Category personal data is defined as personal data consisting of (but not limited to) information as to:
- a) race;
 - b) ethnic origin;
 - c) politics;
 - d) religion;
 - e) trade union membership;
 - f) genetics;
 - g) biometrics (where used for ID purposes);
 - h) health;
 - i) sex life; or
 - j) sexual orientation.
- 3.6 The GDPR rules for special category data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

4. Duties

- 4.1 BTAS will ensure:
- i. The Registrar has responsibility for data protection;
 - ii. Everyone managing and handling personal information understands that they are responsible for following good data protection practice by inclusion in their Terms of Employment or Terms of Appointment;
 - iii. Everyone managing and handling personal information is fully acquainted through induction with the principles of the Regulation;
 - iv. Anyone wanting to make enquiries about handling personal information, whether a member of BTAS or a member of the public, knows what to do;
 - v. Queries about handling personal information are dealt with promptly and courteously and in compliance with the principles under the Regulation;
 - vi. Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing;

- vii. Paper files and other records or documents containing personal/sensitive data are kept in a secure environment (specifically case files and any documents relating to an ongoing matter);
 - viii. Personal data held on computers and computer systems are protected by encryption and/or the use of secure passwords, which where possible change periodically;
 - ix. Individual passwords should be such that they are not easily compromised.
- 4.2 All staff and members of the BTAS disciplinary pool and the Inns' Conduct Committee are to be made fully aware of this policy and of their duties and responsibilities under the Regulation at the time of their recruitment or appointment.
- 4.3 If BTAS decide to transfer personal data outside the EEA, and the recipient is not in a country subject to a Commission 'positive finding of adequacy' nor signed up to the Safe Harbor Scheme, BTAS will need to assess whether the proposed transfer will provide an adequate level of protection for the rights of the data subjects in connection with the transfer/processing of their personal data.
- 4.4 Members of BTAS disciplinary panel and ICC must equally observe paragraph 4.3, and ensure that any e-mail service provider or back-up system they utilise for the receipt or storage of case papers is within the EEA.

5. Disclosure and transfer of personal data

- 5.1 No member of BTAS staff, disciplinary panels or ICC members may disclose any personal/sensitive data unless it has been made clear by the Registrar that they have been authorised to do so.
- 5.2 Personal data must not be transferred unless:
- i. The data subject has given authorisation; and/or,
 - ii. The data subject has made an access request; and/or
 - iii. The Regulation specifically allows the transfer in the circumstances.

6. Destruction of personal data

- 6.1 Personal data must not be held for longer than necessary. When data is destroyed, measures must be taken to ensure that destroyed data cannot be reconstructed.

- 6.2 This applies to all hard copy case / hearing papers issued to panellists or committee members in the discharge of their role, and which must be disposed of by means of BTAS confidential waste collection. No files shall be retained by panellists or committee members.
- 6.3 Personal information or data held electronically in the form of case / hearing papers must be deleted from the PC drive and from any portable or remote storage system as soon as a case is finally concluded. No electronic files shall be retained by panellists or committee members.
- 6.4 Failure to comply with paragraphs 4.4, 6.2 and / or 6.3 may result in the panel or committee member being removed from office.

7. Data subject's access requests

- 7.1 One of the main rights which the Regulation gives to individuals is the right of access to their personal information. Equally the Regulation provides that individual data subject the right to request the destruction of personal data held by BTAS.
- 7.2 The individual data subject must send a subject access request, inquiring about the personal information BTAS holds about them. BTAS will respond to a valid subject access request without undue delay and within one month of receipt, and where appropriate, provide the individual data subject with a copy of the information requested.

8. Data Retention, Storage & Disposal

- 8.1 Further details on how BTAS securely stores and disposes of information and the relevant retention periods are described with the BTAS Data Retention, Storage & Disposal Policy.

9. Review

- 9.1 This policy will be monitored and reviewed annually.