Four Brick Court

Data Protection Policy

Introduction

This Chambers is required to comply with the law governing the management and storage of personal data, which is outlined in the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018.

For this reason, protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of Chambers.

Compliance with the GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office (ICO). This Chambers is accountable to the ICO for its data protection compliance.

Purpose

This policy aims to protect and promote the data protection rights of individuals and of Chambers, by informing members and everyone working for and with Chambers, of their data protection obligations and of Chambers procedures that must be followed in order to ensure compliance with the GDPR.

Scope

This policy applies to all members of chambers, pupils, staff, consultants and any third party to whom this policy has been communicated. *Any breach of the GDPR will be dealt with under our disciplinary policy and may be a criminal offence, in which case the matter will be reported to the appropriate authorities. This policy is applicable to members when they are processing data on and behalf of 4 Brick Court by virtue of their membership of Chambers, where sitting on a Chambers Committee or for other internal matters associated with their membership.*

This policy covers all personal data and special categories of personal data, processed on computers or stored in manual (paper based) files.

Responsibility

Clive Barrett, Senior clerk, is responsible for monitoring Chambers' compliance with this policy.

Everyone in Chambers (and any third party to whom this policy applies to) is responsible for ensuring that they comply with this policy. Failure to do so may result in disciplinary action/termination of third-party contracts.

Data Protection Manager (DPM)

Chambers has appointed the Chambers Senior Clerk, Clive Barrett, as its Data Protection Manager (DPM). This is not a statutory role. His responsibilities within this role include:

- Developing and implementing data protection policies and procedures;
- Arranging periodic data protection training for all staff and members which is appropriate to them;
- Acting as a point of contact for all colleagues, staff and barristers on data protection matters;
- Monitoring Chambers' compliance with its data protection policy and procedures;
- Promoting a culture of data protection awareness;
- Assisting with investigations into data protection breaches and helping Chambers to learn from them;
- Advising on Data Protection Impact Assessments; and
- Liaising with the relevant supervisory authorities as necessary (i.e. the Information Commissioner's Office in the UK).

GDPR

The GDPR is designed to protect individuals and personal data which is held and processed about them by Chambers or other individuals.

The GDPR uses some key terms to refer to individuals, those processing personal data about individuals and types of data covered by the Regulation. These key terms are:

Personal data	Means any information relating to an identified and identifiable natural person **('data subject')** This includes for example information from which a person can be identified, directly or indirectly, by reference to an identifier i.e. name; ID number; location data; online identifiers etc. It also includes information that identified the physical, physiological, genetic, mental, economic, cultural or social identity of a person. For Chambers' purposes, Barristers' clients and Chambers' staff are data subjects (other individual third parties concerning whom we hold personal data about are also likely to be data subjects).
Controller	Means the natural or legal person, public authority, agency or other body who alone or jointly with others, determines the purposes and means of processing the personal data. In effect, this means the controller is the individual, organisation or other body that decides how personal data will be collected and used. For Chambers' purposes, this Chambers is a data controller for certain categories of data.
Processing	Means any operation which is performed on personal data 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. For Chambers' purposes, everything that we do with client information (and personal information of third parties) is 'processing' as defined by the GDPR. This processing will often be in the capacity as a Data Processor on behalf of a Barrister as a Data Controller.
Special categories of personal data	Means personal data revealing: a) racial or ethnic origin; b) political opinions;

c) religious or philosophical beliefs;
d) trade-union membership;
e) the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person;
f) data concerning health or data concerning a natural person's sex life or sexual orientation

N.B. data relating to criminal convictions and offences is not included within the special categories. However, there are additional provisions for processing this type of data (see Regulation 10 of GDPR)

Data Protection Principles

The GDPR is based around 8 principles which are the starting point to ensure compliance with the Regulation. Everybody working in, for and with Chambers must adhere to these principles in performing their day-to-day duties. The principles require Chambers to ensure that all personal data and sensitive personal data are:

1. Processed lawfully, fairly and in a transparent manner in relation to the subject ('**lawfulness**, **fairness** and **transparency**')
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**')
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**')
4. 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 ('**accuracy**')
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed ('**storage limitation**')
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('**integrity and confidentiality**')

Chambers must be able to demonstrate its compliance with (1)– (6) above ('**accountability**').

Consent

We understand 'consent' to mean that it has been explicitly and freely given, and it is a specific, informed and unambiguous indication of the Data Subject's wish that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The Data Subject can withdraw their consent at any time.

We also understand 'consent' to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

Consent cannot be inferred from non-response to a communication. As Data Controller, we must be able to demonstrate that consent, where necessary, was obtained for the processing operation.

For Sensitive Personal Data, explicit written consent of Data Subjects must be obtained unless an alternative legitimate basis for processing exists.

Where we provide online services to children under the age of 16, parental or custodial authorisation must be obtained.

Processing personal data and sensitive personal data

You must process all personal data in a manner that is compliant with the GDPR, in short, this means you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

You must ensure that you are aware of the difference between personal data and special categories of personal data and ensure that both types of data are processed in accordance with the GDPR.

The conditions for processing special categories of personal data that are most relevant to our Chambers are:

- Explicit consent from the data subject;
- The processing is at the instruction of a Barrister who is the Data Controller of that personal data;
- The processing is necessary for the purposes of carrying out Chambers' obligations in respect of employment and social security and social protection law;
- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing relates to personal data that has already been made public by the data subject; or
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

If you have any concerns about processing personal data, please contact Clive Barrett, who will be happy to discuss matters with you.

Rights of the data subject

The GDPR gives rights to individuals in respect of the personal data that any organisations hold about them. Everybody working for Chambers must be familiar with these rights and adhere to Chambers' procedures to uphold these rights.

These rights include:

- Right of information and access to confirm details about the personal data that is being processed about them and to obtain a copy;
- Right to rectification of any inaccurate personal data;
- Right to erasure of personal data held about them (in certain circumstances);
- Right to restriction on the use of personal data held about them (in certain circumstances);
- Right to portability – right to receive data processed by automated means and have it transferred to another data controller;
- Right to object to the processing of their personal data.

If anybody receives a request from a data subject (a client or other third party concerning whom we hold personal data) to exercise any of these rights, the request must immediately be referred Clive Barrett**, Data Protection Manager**, or to Jayne Harrill**, Head of Chambers**, in his absence.

Data Subjects may make Subject Access Requests relating to their personal data. Our Subject Access Request Policy describes how we will ensure that our response to the request complies with the requirements of the GDPR.

Our DPO/DPL is responsible for responding to requests for information from Data Subjects within one calendar month in accordance with our Subject Access Request Policy. This can be extended to two months for complex requests in certain circumstances. If we decide not to comply with the request, the DPO/DPL must respond to the Data Subject to explain our reasoning and inform them of their right to complain to the ICO and seek judicial remedy.

Data Subjects have the right to complain to us about the processing of their personal data, the handling of a Subject Access Request and to appeal against how their complaints have been handled.

Accuracy of Data

Our DPM is responsible for ensuring that all employees are trained in the importance of collecting *accurate data and maintaining it.*

Employees are required to notify the Senior Clerk of any changes in their personal circumstances which may require personal records be updated accordingly.

Our DPM is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

Our DPM is responsible for making appropriate arrangements where third-party organisations may have been passed inaccurate or out-of-date personal data to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

Security of Data

All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security as set out in our Data Security Policy.

No less than annually our DPM will carry out a risk assessment taking into account all the circumstances of our data controlling and processing operations.

In determining appropriateness of all technical and organisational security measures, the DPM will consider the extent of possible damage or loss that might be caused to individuals (e.g. staff, clients or members) if a security breach occurs, the effect of any security breach on our organisation itself, and any likely reputational damage, including the possible loss of customer trust.

It is strictly prohibited to remove personal data from our premises for any reason other than carrying out legitimate processing activities.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft, or damage to personal data and the precautions that must be taken are set out in our Data Security Policy and Remote Working Policy.

All employees are responsible for ensuring that any personal data that we hold and for which they are responsible is kept securely and is not, under any condition, disclosed to any third party unless that third party has been specifically authorised by us to receive that information and has entered into a Data Sharing Agreement.

Disclosure of Data

All requests to provide personal data must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Manager.

We must ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and, in certain circumstances, the Police. All employees should exercise caution when asked to disclose personal data held on another individual to a third party.

Retention and Disposal of Data

We shall not keep personal data in a form that permits identification of Data Subjects for a longer period than is necessary in relation to the purpose(s) for which the data was originally collected.

The retention period for each category of personal data is set out in our Retention and Disposal Policy.

Personal data will be retained in line with our Retention and Disposal Policy and, once its retention date is passed, it must be securely destroyed as set out in this policy.

On at least an annual basis, our DPM will review the retention dates of all the personal data processed by our organisation and will identify any data that is no longer required. This data will be securely archived, deleted or destroyed in line with our Retention and Disposal Policy.

Where personal data is archived it will be [minimised/encrypted/pseudonymised] in order to protect the identity of the Data Subject in the event of a data breach.

Our DPM must specifically approve any data retention that exceeds the retention periods defined in our Retention and Disposal Policy, and must ensure that the justification is clearly identified and recorded.

We may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the Data Subject. Any such retention must be approved in advance by the DPM.

Confidentiality and data sharing

The barristers and Chambers must ensure that they share personal information with other individuals or organisations only where they are permitted to do so in accordance with data protection law.

Wherever, possible you should ensure that you have the client's (or other data subject's) consent before sharing their personal data, although, it is accepted that this will not be possible in all circumstances, for example if the disclosure is required by law. Any further questions around data sharing should be directed to Clive Barrett.

Data Protection Impact Assessments (DPIAs)

DPIAs are required to identify data protection risks; assess the impact of these risks; and determine appropriate action to prevent or mitigate the impact of these risks when introducing or making significant changes to systems or projects involving the processing of personal data.

In simpler terms, this means thinking about whether Chambers is likely to breach the GDPR and what the consequences might be, if Chambers uses personal data in a particular way. It is also about deciding whether there is anything that Chambers can do to stop, or at least minimise the chances of any of the potential problems identified, from happening.
DPIAs will be undertaken by **Clive Barrett, Data Protection Manager**, or other designated persons.

International Data Transfers
Under GDPR, transfers of personal data outside of the European Economic Area can only be made if specific safeguards exist.

No employee is authorised to transfer personal data internationally until the DPO/DPL has confirmed in writing that we have appropriate safeguards in place.

Data Processed Register
We have established a Data Processed Register that records:

- *each type of personal data;*
- *why it is collected;*
- *the lawful grounds for processing;*
- *where it is held;*
- *the Responsible Person for the data;*
- *its Review Date; and*
- *how it is kept accurate.*

Breaches

A data protection breach is defined 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".

Breaches will be reported to the Information Commissioner's Office (ICO) by the person who created the breach within 72 hours after having become aware of the breach unless, Chambers is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Everybody working in, for and with Chambers has a duty to report any actual or suspected data protection breach without delay to **Jayne Harrill Head of Chambers** (Jayne.harrill@4bc.co.uk) and **Clive Barrett**, **Data Protection Manager** (clive.barrett@4bc.co.uk).

Hard copies of this policy and Chambers' **Data Protection Breach Reporting Procedure** (DPBRP) are located in the **Chambers Library** on First Floor West and in the **Clerks Room** on Ground Floor East. Electronic versions of both documents have been emailed to every member of chambers, pupil, and staff in any event.

The DPBRP explains how to report a breach to the ICO.

The Data Protection Manager will maintain a central register of the details of any data protection breaches.

Complaints

Complaints relating to breaches of the GDPR and/or complaints that an individual's personal data is not being processed in line with the data protection principles should be referred to **Jayne Harrill**, **Head of Chambers** and **Clive Barrett**, **Data Protection Manager** without delay.

Penalties

It is important that everybody working for Chambers understands the implications for Chambers if we fail to meet our data protection obligations. Failure to comply could result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension/ withdrawal of the right to process personal data by the ICO;
- Loss of confidence in the integrity of the business's systems and procedures;
- Irreparable damage to the business's reputation.

Note: Chambers could be fined up to €20,000,000, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.