Data Protection Policy

Guidance Notes

You should ensure this policy is written and regularly reviewed.

A chambers' Data Protection Policy is a completely different policy from your own. It does not protect you or your practice; it protects chambers in its own role as a data controller. Do not assume because your chambers has a Data Protection Policy that you do not need one.

2021 Update

This template has been reviewed and additional information has been included:

Introduction: An additional role setting out your role as a processor for chambers' data.

Data Protection Law: Additional information relating to the processing of special category data and criminal offence data have been included. Where this is relevant to your practice this should be inserted into your existing policy.

An additional section on handling Data Breaches has also been included.

This template has also been amended to reference the transfer of data out of the UK rather than the EEA.

DATA PROTECTION POLICY OF:

Previn Jagutpal

4 Brick Court

ICO Registration Number: Z1067590

Policy became operational on: 14th June 2022

Next review date: 14th June 2025

Data Protection Policy

Introduction

I need to gather and use personal data about individuals in the course of my practice as a barrister, both for the provision of my professional services and to manage my practice.

I will process personal data relating to a range of individuals. In my capacity as data controller this may include, but is not limited to:

- Clients (whether instructed by a law firm or by direct access);
- Suppliers and support services, including 4 Brick Court and its employees;
- Business contacts;
- Employees; and
- Other people I have a professional relationship with or may need to contact.

On occasion I may sit on a chambers committee or have access to chambers-controlled personal information, e.g. staff information. Where I do so I will be acting in my capacity as data processor for chambers and will process personal data shared with me by chambers.

This policy describes how this personal data must be collected, handled and stored to meet my data protection standards and to comply with the law.

Why this policy exists

This Data Protection Policy exists to ensure that I and any staff I may employ:

- Comply with data protection law and implement robust data protection policies and procedures within their practice;
- Protect the rights of all data subjects;
- Am open about how I store and process individuals' data;
- Protect my practice from the risks of a data breach.

Data protection law

The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 describe how organisations must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The UK GDPR is underpinned by six important principles. They say that personal data must be:

1. Processed lawfully, fairly and transparently;
2. Collected for specific, explicit and legitimate purposes;
3. Adequate, relevant and limited to what is necessary for processing;
4. Accurate and, where necessary, kept up to date;
5. Kept in a form such that the data subject can be identified only as long as is necessary for processing; and
6. Processed in a manner that ensures appropriate security of the personal data.

Processing personal data and sensitive personal data

Where I am processing personal data, I must do so in a way which is compliant with the UK GDPR and the principles set out above and which demonstrates my accountability under the legislation.

I must be able to demonstrate:

· a lawful basis for processing personal data;
· transparency with data subjects about how I intend to use their personal data
· that I have processed personal data only in ways the data subject would reasonably expect; and
· make sure I do not do anything unlawful with the data.

Where I am processing special category data, I must ensure that I can evidence an exemption which allows me to process such data. The conditions most relevant to my practice are:

- The processing is necessary to protect the vital interests of the data subject or another person.
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever processing is taking place to enable courts to act in their judicial capacity (including members who act in judicial capacities such as a deputy judge or appointed person).
- Explicit consent from the data subject.

Where I am processing criminal offence data, I must ensure that I can evidence an exemption which allows me to process such data. The conditions most relevant to my practice are:

- Explicit consent from the data subject.
- The processing is necessary to protect the vital interests of the data subject or another person.

- The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), to obtain legal advice or to establish, exercise or defend legal rights.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the UK GDPR and Data Protection Act 2018.

People, risks and responsibilities

Policy scope

People

This policy applies to:

- Any employee of my practice such as support staff (e.g. typists, secretary) as well as trainees, volunteers and work experience students. It does not include chambers staff who are governed by the chambers' own policy.

- All contractors, individuals, suppliers and other relevant parties working on behalf of my practice.

- All data my practice holds relating to identifiable individuals. This can include but is not limited to:

    - Name
    - Email address
    - Phone number
    - Address
    - Payment or bank details
    - Date of birth
    - Next of kin details
    - Details pertaining to education and employment
    - Information on your background & current circumstances
    - Financial information;

- Special category personal data that reveals:

    - Racial or ethnic origin
    - Political opinions
    - Religious and philosophical beliefs
    - Trade union membership
    - Genetic data
    - Biometric data for the purpose of uniquely identifying a natural person
    - Data concerning health
    - Sex life and sexual orientation.

Personal information relating to individuals employed by an organisation, company or public body with whom I work is also included.

Responsibilities

Both I and any employees of my practice have responsibility for ensuring data is collected, stored and handled appropriately and in compliance with the law.

Data Protection Policy information

I will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information;
- Meet my legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, but only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements;
- Ensure the quality and accuracy of information used;
- Ensure appropriate retention and disposal of information;
- Ensure that the rights of people about whom information is held can be fully exercised under the UK GDPR. These include:
    - The right to be informed
    - The right of access
    - The right to rectification
    - The right to erase
    - The right to restrict processing
    - The right to data portability
    - The right to object, and
    - Rights in relation to automated decision-making and profiling;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred outside the UK without suitable safeguards;
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information;
- Set out clear procedures for responding to requests for information;
- Take appropriate steps to complete due diligence and enter into contractual arrangements with data processors and controllers where personal data is shared;
- Ensure all regulatory requirements are satisfied when processing special category data and criminal information.

Data storage

All personal information or data processed within my practice will be stored securely and will only be accessible to authorised staff and data processors that I appoint.

Information will be stored for only as long as it is needed or as required by statute, for compliance with professional regulatory obligations, professional indemnity requirements and in compliance with my Data Retention Policy. All personal data will be disposed of appropriately and securely in accordance with the Data Retention and Disposal Policy and Data Security Policy.

Where personal data has been shared with third parties for the purposes of providing my services and managing my practice, such data will be retrieved from the third party (data processor) or directions will be given to the third party about safe disposal of such data in accordance my data retention policy.

I will ensure all personal data is non-recoverable from any computer system I use or dispose of.

This policy should also be read in conjunction with the Data Security Policy and Data Retention and Disposal Policy of my practice.

Data access and accuracy

All data subjects have the right to access the information I hold about them, except where specific exemptions apply to me as a legal professional. I will also take reasonable steps to ensure that this information is kept up to date.

In addition, I will ensure that:

- All employees of mine, or third parties with whom I work:
    - understand that they are contractually responsible for following good data protection practice;
    - are appropriately trained to do so and are aware of the process for managing requests for access to data by data subjects; and
    - are appropriately supervised.

- Any data subject who wishes to make enquiries about how their personal information has been processed knows how to make this request.
- Where required, I will work with other parties to facilitate and respond to such requests for data.
- I will ensure that where I share data with a third party, they are contractually bound to assist with requests from data subjects seeking access to their data.

Disclosure

I may share data with third parties, including, but not limited to, instructing solicitors, other agencies such as government departments and other relevant parties. Where this occurs, I will ensure that where appropriate a Data Sharing Agreement is in place.

I will ensure that data will not be shared outside the UK or with unauthorised parties without my specific permission. Data subjects will be made aware in most circumstances about how and with whom their information will be shared.

There are circumstances where the law allows the barrister to disclose data (including sensitive data) *without* the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State;
b) Protecting vital interests of an individual/data subject or other person;
c) The individual/data subject has already made the information public;
d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights;
e) Monitoring for equal opportunities purposes – i.e. race, disability or religion;
f) Providing a confidential service where the individual/data subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill individuals/data subjects to provide consent signatures.

Data protection training

I will ensure that I and any individuals employed by me are appropriately trained in data protection annually.

If new members of staff commence work with me, they will be provided with data protection training within [the first month] of employment.

I will keep a register of all training completed by me or any employees for ICO audit purposes.

Breaches of personal data

In the event of a data protection breach, which 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", I will undertake the following steps:

- I will instigate necessary investigation as per the guidance in the Data Breach and Crisis Management plan.

- Where it is determined that the breach has met with the required threshold and is likely to result in a risk to the rights and freedoms of the data subjects involved, I will report the breach to the Information Commissioner's Office (ICO

without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.

- Where it is assessed that the data subjects should be informed of the data breach, I will take the relevant steps to advise the affected parties.

- I will make an assessment whether the data breach merits a report to the Bar Standards Board in accordance with their guidance and code of conduct.

Complaints

Complaints relating to breaches of the UK 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 myself.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the UK GDPR and Data Protection Act 2018.

Non-conformance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

In case of any queries or questions in relation to this policy, please contact me as Data Protection Lead: