GDPR Data Protection Policy

New Bailey Chambers and its members are Data Controllers and processors under the General Data Protection Regulations and are registered with the Information Commissioner's Office as a Data Controllers.

This policy applies to all the personal data that Chambers holds relating to identifiable individuals.

New Bailey Chambers recognises that it controls and processes personal data and we are therefore responsible for compliance with the GDPR in relation to the personal data that we hold. We recognise and accept this as our responsibility.

Background to the General Data Protection Regulation (GDPR)

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the UK's Data Protection Act 1998. Its purpose is to protect the "rights and freedoms" of living individuals in relation to their personal data.

New Bailey Chambers follows the data protection regulations and laws as set out in The UK General Data Protection Regulation and the Data Protection Act 2018. Their purpose is to protect the "rights and freedoms" of living individuals in relation to their personal data.

Policy Statement

The Head of Chambers, management, employees and members of New Bailey Chambers are committed to compliance with all relevant EU and UK laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with the General Data Protection Regulation (GDPR).

The GDPR and this policy apply to all of our personal data processing functions, including those performed on customers', clients', employees', and suppliers' personal data, and any other personal data we process from any source.

Laura Armstrong (Senior Clerk) is our designated Data Protection Officer (DPO) who is overseen by Augustine Iro (Head of Chambers). They are responsible for all data protection matters.

This policy applies to all employees (permanent and temporary), agency, and contract staff. Any breach of the GDPR will be dealt with under our disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

It is also applicable to Members when they are processing Chambers data on and behalf of New Bailey Chambers by virtue of their membership of Chambers, where sitting on a Chambers Committee or for other internal matters associated with their membership.

Partner organisations and third parties (sub-processors) working with or for us which have or may have access to personal data will be expected to adhere to all obligations imposed by data protection legislation. No third party may access personal data held by us without having first entered into a Data Sharing Agreement which imposes on the third party obligations no less onerous than those to which we are committed, and which gives us the right to audit compliance with the Agreement.

DEFINITIONS AND INTERPRETATION

a. **GDPR** means the UK General Data Protection Regulation.

b. **'New Bailey Chambers'** and **'Chambers'** shall refer to our business operations as a whole, our Barristers members and our staff.

c. The terms **'Personal Data', 'Controller'**, **'Processor'** and **'Personal Data Breach'** shall have the same meaning as contained within the GDPR and should be interpreted as such.

d. The term **'DPO'** shall refer to New Bailey Chamber's Data Protection Officer.

e. **'Sub-processor'** shall be interpreted to mean any person or company contracted by the Processor to process or hold personal data on behalf of New Bailey Chambers.

f. References to **'processing'** shall be understood to relate to the processing referred to within this policy.

Definitions

Data Protection Principles

All processing of personal data must be conducted in accordance with the Data Protection Principles as set out in the GDPR and outlined below. Our policies and procedures are designed to ensure compliance with these Principles.

Principle 1

Personal data must be processed lawfully, fairly, and transparently

Lawful – we need to identify a lawful basis before we can process personal data, for example, consent.

Fairly – in order for processing to be fair, we have to make certain information available to Data Subjects. This applies whether the personal data was obtained directly from Data Subjects or from other sources.

Transparently – the GDPR includes rules on giving privacy information to Data Subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

Principle 2

Personal data can only be collected for specific, explicit, and legitimate purposes

The data we obtain for specified purposes must not be used for a purpose that is incompatible with those formally notified to the ICO as part of our GDPR register of processing.

Principle 3

Personal data must be adequate, relevant, and limited to what is necessary for processing

We cannot collect information that is not strictly necessary for the purpose for which it is obtained.

Principle 4

Personal data must be accurate and, where necessary, kept up to date.

Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay. Data that is stored by us must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

Principle 5

Personal data must be kept in a form such that the Data Subject can be identified only as long as is necessary for processing.

We should only hold personal data for as long as we need it.

Principle 6

Personal data must be 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.

Demonstrating Accountability

The GDPR includes provisions that promote Accountability and Governance. These complement the GDPR's transparency requirements. Accountability requires us to demonstrate that we comply with the GDPR Principles.

We will demonstrate compliance with the GDPR Principles by implementing and adhering to data protection policies, implementing technical and organisational measures, as well as adopting techniques such as Data Protection by Design, Data Protection Impact Assessments, breach notification procedures and incident response plans.

Data Subjects' Rights

The GDPR provides the following rights for individuals in relation to their personal data:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure

5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

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 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 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.

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 13, parental or custodial authorisation must be obtained. At present we do not provide online services to children.

Collection of Data

All data collection forms (electronic and paper-based), including data collection requirements in new information systems, must include a fair processing statement or a link to our Privacy Notice and be approved by the DPO.

Accuracy of Data

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

Employees are required to notify Chamber's Management Committee of any changes in their personal circumstances which may require personal records be updated accordingly.

Our DPO 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 DPO 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 DPO 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 DPO 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 Officer.

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 DPO 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 DPO 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 DPO.

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 has confirmed that appropriate safeguards are 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.

Data Protection Impact Assessments (DPIA)

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of living peoples, we shall, prior to the processing, carry out a Data Protection Impact Assessment of the envisaged processing operations. All DPIAs should be led by or overseen by the DPO.

Where, as a result of a DPIA it is clear that we are about to commence processing of personal data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not we may proceed must be referred to senior management for approval to proceed.

Our DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, refer to the ICO for guidance and advice.