THE HONOURABLE SOCIETY OF THE
MIDDLE TEMPLE

DATA PROTECTION POLICY

June 2024

Contents

Introduction

This data protection policy ("policy") sets out how The Honourable Society of the Middle Temple ("we", "our", "us", "the Inn") handles the personal data of our employees, members, customers, suppliers, and other third parties. It explains how the Inn meets its legal obligations with regards to data protection under UK legislation. This is primarily based on the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). For the purposes of data protection law, The Honourable Society of the Middle Temple is a data controller and is registered with the Information Commissioner's Office (ICO).

This policy applies to all personal data that the Inn processes regardless of the media on which that personal data is stored or who the data subject is.

This policy sets out what is expected from the Inn and its staff in order to comply with data protection law. This policy applies to all staff, whether permanent, temporary, or casual. All staff are expected to read, understand, and comply with this policy when processing personal data on the Inn's behalf and attend training on its requirements. Related policies and privacy guidelines are available to help staff interpret and act in accordance with this policy. Any breach of this policy may result in disciplinary action being taken.

Definitions

For definitions of the technical terms used in this policy please refer to the Glossary of terms at the end of this document.

Data protection principles

The Inn regards the lawful and correct treatment of personal data as very important to successful working and to maintaining the confidence of those with whom we deal. To this end, the Inn adheres to Article 5 of the UK GDPR which sets out the key principles for processing personal data.

Specifically, 5(1) requires 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;*

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;*

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;*

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.*

Article 5(2) adds that:

Appropriate measures and records should be in place to be able to demonstrate compliance with the above principles.

Personal data

The UK GDPR definition of personal data is for any information relating to an identified or identifiable natural person – i.e. living individuals. Data that is pseudonymised is covered, however, anonymised data is not, providing that it cannot be reversed.

The Inn collects, uses, and stores personal data on a range of individuals, these are the data subjects. This includes, but is not limited to, members, employees, tenants, contractors, and clients. Examples of personal data that the Inn processes include names, addresses, email addresses, phone numbers, membership numbers, financial information, payroll data, photographs, and video records. This personal data may be collected in a number of different ways, for example, paper-based or online forms, emails, or over the telephone.

The legislation also defines special category personal data (previously referred to as sensitive personal information), which is information related to:

- race or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- health data
- sexual history and/or sexual orientation

Criminal offence data is also afforded extra protection under the legislation.

The personal data that the Inn collects and uses is set out in privacy notices on our website: https://www.middletemple.org.uk/about-us/data-protection/privacy-policies-and-notices

Use of personal data

In order to comply with principle 5(1)(a) above, the Inn must have a specified lawful purpose for processing personal data. This is to ensure that we process personal data fairly and without adversely affecting the data subject.

The lawful bases for processing are set out in Article 6 of the UK GDPR. Some examples of lawful bases for processing personal data most commonly used by the Inn include:

- the data subject has given their consent
- the processing is necessary for the performance of a contract with the data subject
- to meet our legal compliance obligations
- to protect the data subject's vital interests

- to pursue the Inns legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the data subject

Individuals should always be made aware that their personal data is being processed, and for what purpose.

Use of special category personal data

The Inn may collect special category personal data in some cases. For example, in order to ensure that staff recruitment or access to the Bar is equally open to all.

Special category data requires more protection because it is sensitive. In order to process this data, the Inn must identify both a lawful basis under Article 6 of the UK GDPR (as above) and a separate condition for processing under Article 9.

The Article 9 conditions for processing special category data are:

(a) Explicit consent

(b) Employment, social security, and social protection (if authorised by law)

(c) Vital interests

(d) Not for profit bodies

(e) Made public by the data subject

(f) Legal claims or judicial acts

(g) Reasons of substantial public interest (with a basis in law)

(h) Health or social care (with a basis in law)

(i) Public health (with a basis in law)

(j) Archiving research and statistics (with a basis in law)

If the Inn uses conditions (b), (h), (i), or (j) we must also meet the associated condition set out in Part 1 of Schedule 1 of the DPA 2018. If we are relying on condition (g) we also need to meet one of the conditions set out in Part 2 of Schedule 1 of the DPA 2018.

Data collection

When collecting personal data, the Inn will ensure that the data subject:

- clearly understands why the personal data is needed
- understands what it will be used for
- understands which of the lawful bases for processing (see above) the Inn is relying on

Disclosures and sharing personal data

The Inn may need to share data externally. For example, with local authorities, HMRC, funding bodies, service providers that the Inn uses, and other agencies connected with the Bar, such as the other Inns of Court, the Bar Council, the Circuits, and Specialist Bar Associations.

Generally, we will not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

Inn staff will only share personal data with another employee if the recipient has a job-related need to know the personal data. For external data sharing, where applicable, third parties are required to sign a data sharing agreement with the Inn to ensure that they agree to comply with the required data security standards, policies, and procedures and that they have put adequate security measures in place.

Details of data sharing can be found in the Inn's privacy notices.

Data protection law restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by data protection law is not undermined.

The Inn will only transfer personal data outside the UK if one of the following conditions applies:

- The country or territory is covered by UK 'adequacy regulations', i.e. the country has been assessed as providing 'adequate' protection for people's rights and freedoms about their personal data. Examples of countries that are covered by adequacy regulations include, the European Economic Area (EEA) countries, New Zealand, and Switzerland. For a full list the ICO website should be consulted.

- Transfer to the USA is covered by a UK-US data bridge that came into force on 12 October 2023. The Inn can transfer personal data to certified organisations in the USA under this agreement.

- Appropriate safeguards are in place, such as binding corporate rules (BCR), standard contractual clauses, an approved code of conduct, or a certification mechanism, a copy of which can be obtained from the Data Protection Officer (DPO).

- The data subject has provided explicit consent to the proposed transfer after being informed of any potential risks.

- The transfer is necessary for one of the other reasons set out in data protection law, including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise, or defend legal claims, or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

Data storage and security

The Inn takes all necessary steps to ensure that personal data is treated securely and in accordance with this policy. All of the Inn's personnel are personally responsible for maintaining confidentiality with regard to personal data and ensuring that such personal data is processed only for the specified purposes for which it is collected. The Inn provides continuing education and training to its personnel about their obligations under this policy and

data protection law. Additionally, only certain personnel members will have access to personal data in order to be able to carry out their work roles.

Personal data will only be stored for as long as it is needed or required and will be disposed of appropriately.

Personal data is stored on secure servers, both at the Inn and at our approved third-party locations consistent with the Inn's IT management and business continuity plans. No Personal Data is held in offsite servers outside the EEA.

A personal data breach is a breach in security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Inn has procedures in place to deal with a personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential personal data breach.

Data subject rights

Data subjects have rights under data protection law in relation to their personal data.

All data subjects have the right to access the personal data that the Inn holds about them. The Inn will also take reasonable steps to ensure that this personal data is kept up to date by regularly asking data subjects if there have been any changes to their personal data.

Data subjects also have the right to:

- request correction of their personal data
- request erasure of their personal data
- object to processing of their personal data
- request restriction of processing of their personal data
- request transfer of their personal data
- withdraw consent

Data subjects can exercise any of the rights set out above by contacting the Inn's DPO. Requests can be made either verbally or in writing, including via social media. Staff are required to make the DPO aware of any requests made to them to ensure that they are dealt with within required statutory time frames.

Data deletion and destruction

In accordance with data protection law, the Inn retains personal data for no longer than is required for its processing as set out in applicable privacy notices. In particular, the Inn will not keep personal data in a form that permits the identification of the data subject for longer than is needed for the legitimate business purpose or purposes for which we originally collected it

including satisfying any legal, accounting, or reporting requirements.

The Inn's retention schedules are available to staff on the Intranet to give guidance on the length of time that certain personal data must be retained before it is deleted and destroyed.

Record keeping

Data protection law requires the Inn to keep and maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents.

These records include the name and contact details of the Inn and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of personal data, personal data storage locations, personal data transfers, retention periods, and a description of the security measures in place.

Accountability

In order to demonstrate compliance with the UK GDPR's Accountability principle, the Inn is required to put in place appropriate technical and organisational measures. These include adopting and implementing data protection polices; taking a 'data protection by design and by default' approach; maintaining documentation of our processing activities; recording and, where necessary, reporting personal data breaches; and putting written contracts in place with organisations that process personal data for us.

'Data protection by design and default' means that the Inn must integrate data protection into its processing activities and business practices from the design stage, right through the lifecycle. We must assess what privacy by design measures can be implemented on all programmes, systems, or processes that process personal data.

The Inn also conducts Data Protection Impact Assessments (DPIAs) in respect to high-risk processing. This is in order to help identify and minimise the data protection risks of a project.

Practical implications

In order to ensure compliance with the data protection principles and data protection legislation, the Inn and its staff will, through appropriate management, and strict application of criteria and controls:

- Ensure that there is a suitably qualified DPO employed by the Inn (as set out in this policy) accountable for data privacy
- Implement data protection by design when processing personal data
- Complete Data Protection Impact Assessments (DPIAs) where processing presents a high risk to the rights and freedoms of data subjects
- Integrate data protection into internal documents including this policy, related policies, privacy guidelines, and privacy notices

- Ensure that everyone processing personal data is appropriately trained to do so, and maintain a record of training attendance
- Ensure that everyone processing personal data is appropriately supervised
- Regularly review and audit the way the Inn holds, manages and uses personal data
- Ensure that there are lawful grounds for using personal data
- Ensure that the use of the data is fair and meets one of the specified conditions
- Only use special category personal data if it is absolutely necessary
- Ensure that individuals are aware at the time of collection how their personal data will be used
- Ensure that personal data is only used for the purpose it was collected for and that the minimum amount necessary is collected
- Keep personal data accurate and up to date
- Use the Inn's retention schedules to ensure data is only kept for as long as is necessary
- Ensure that individuals can manage their own communications preferences
- Ensure that the rights of data subjects can be fully exercised
- Ensure that personal data is secured by appropriate, technical, and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage

Roles and Responsibilities

Adhering to data protection legislation and maintaining confidentiality applies to everyone at the Inn. The Inn will take all necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice. New employees will receive training and be required to sign this Data Protection Policy as part of their induction. Volunteers and Members who may also come into contact with personal data will also be asked to sign the policy.

All employees, volunteers and contractors have a responsibility to:

- Observe all guidance and policies in relation to obtaining, using and disclosing personal data and special category personal data
- Obtain and process personal data and special category personal data only for specified purposes
- Only access data that is specifically required to carry out their activity or work
- Record data correctly

- Ensure that any data that is held is kept secure
- Ensure that personal data and special category personal data is not disclosed in any form to any unauthorised third party
- Ensure that secure methods are used for sending personal data and special category personal data
- Read and sign the Data Protection Policy, directing any questions to the Data Protection Officer

Failure to adhere to this policy could result in disciplinary action.

All managers are responsible for:

- Determining what personal data they are responsible for and ensuring that the data is adequately secure, access is controlled and that the data is only used for the intended purposes
- Providing clear messaging to their teams about data protection requirements and measures
- Ensuring personal data is only held for the purpose intended
- Ensuring personal data is not communicated or shared for non-authorised purposes
- Ensuring personal data is password protected when transmitted or appropriate security measures are taken to protect it

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing this policy and, as applicable, developing related policies and privacy guidelines. If you have any questions about the operation of this policy or data protection law or if you have any concerns that this policy is not, or has not been, followed please contact the DPO.

The DPO is responsible for:

- Ensuring compliance with data protection legislation
- Communication with the ICO regarding processing of personal data and reporting of breaches
- Providing guidance and advice to employees in relation to compliance with legislative requirements
- Auditing data protection arrangements annually
- Ensuring those handling personal data are aware of their obligations by providing training and guidance

The DPO should always be contacted in the following circumstances:

- If you are unsure of the lawful basis which you are relying on to process personal data;
- If you need to rely on consent and/or need to capture explicit consent;
- If you are unsure about the retention period for any personal data being processed;
- If you are unsure about what security or other measures you need to implement to protect personal data;
- If there has been a personal data breach;
- If you are unsure on what basis to transfer personal data outside of the UK;
- If you receive a request concerning any rights under data protection law that are invoked by a data subject;
- Whenever you are engaging in a significant new, or change in, processing activity that is likely to require a DPIA or plan to use personal data for purposes other than those it was collected for;
- If you plan to undertake any activities involving automated processing including profiling or automated decision-making;
- If you need help complying with applicable law (including data protection law) when carrying out direct marketing activities; or
- If you need help with any contracts or other areas in relation to sharing personal data with third parties.

In the Data Protection Officer's absence, advice can be sought from the ICO https://ico.org.uk/

Data protection management

This policy will be reviewed periodically and updated as necessary to reflect best practice in data management, security, and control, and to ensure compliance with any changes or amendments made to data protection law.

This policy does not override any data protection law.

This version was last updated on 26 June 2024.

In case of any queries or questions in relation to this policy please contact the Inn's DPO:

Data Governance Manager
The Honourable Society of the Middle Temple
Ashley Building, Middle Temple Lane, London
EC4Y 9BT

Email: **Data.Protection@middletemple.org.uk**

Privacy policies

The Inn has a number of privacy policies relating to the different areas of its work and an Appropriate Policy Document. These can be found on the Inn's website: https://www.middletemple.org.uk/about-us/data-protection/privacy-policies-and-notices

Glossary of terms

The following list of definitions is intended to aid in the understanding of this policy. If you have any questions regarding these definitions, then please get in touch with the Inn's DPO.

Consent – an agreement that must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.

Data controller – the person/entity who decides when, why, and how personal data is processed. The Inn is the data controller of all personal data relating to its personnel and personal data used in its business for its own operational purposes.

Criminal convictions data – personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Privacy Impact Assessment (DPIA) – tools and assessments used to identify and reduce risks associated with processing activity.

Data protection law – the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018 ('DPA2018'), and any other privacy or data protection laws (including any statutes, regulations, by-laws, ordinances, mandatory codes of conduct, or rules of common law or equity).

Data Protection Officer (DPO) – the person(s) responsible for ensuring that the Inn follows this policy, related policies, and privacy guidelines, and complies with data protection law.

Data subject/service user – an individual, the personal data of which is being held and/or processed by the Inn (for example, a member, a client, an employee, or a supporter).

DPA 2018 – the Data Protection Act 2018, which (among other functions) assists in transposing the GDPR into English law.

EEA – the 28 countries of the EU, and Iceland, Liechtenstein, and Norway.

'Explicit' consent – a freely given, clear, specific, and informed agreement that is not just an action, by a data subject or service user to the processing of personal data about him/her. Explicit consent is needed for processing special category personal data.

Information Commissioner – the UK supervisory authority responsible for implementing and overseeing data protection law.

Personal data – any information identifying a data subject or information relating to a data subject who is identifiable (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name,

email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Breaches may be accidental or deliberate.

Privacy notices (also referred to as fair processing notices or privacy policies) – separate notices setting out information provided to data subjects when the Inn collects personal data. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, an employee privacy notice) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Processing – any activity that involves the use of personal data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Pseudonymised or Pseudonymisation – replacing information that directly or indirectly identifies an individual with one or more artificial identifier or pseudonym so that the person, to whom the data relates, cannot be identified without the use of additional information that is kept separately and securely.

Special categories of (or special category) personal data – information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

UK General Data Protection Regulation (UK GDPR) – the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).