



1 DATA PROTECTION POLICY

This document sets out the Firm's policy on the protection of information relating to employees, workers, contractors, volunteers and interns (referred to as employees). Protecting the confidentiality and integrity of personal data is a critical responsibility that the Firm takes seriously at all times. The Firm will ensure that data is always processed in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR).

1.1 KEY DEFINITIONS

1.1.1 Data Processing

Data processing is 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.

1.1.2 Personal Data

Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Firm possesses or can reasonably access. 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.

1.1.3 Sensitive Personal Data

Sensitive personal data is a special category of information which relates to a data subject's 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.

It also includes personal data relating to criminal offences and convictions.

1.1.4 Privacy Notice

This policy, together with the table of employee data, a copy of which is available from the Group HR Manager, constitutes a privacy notice setting out the information the Firm holds about employees, the purpose for which this data is held and the lawful basis on which it is held. The Firm may process personal information without employees' knowledge or consent, in compliance with this policy, where this is required or permitted by law.

If the purpose for processing any piece of data about employees should change, the Firm will update the table of employee data with the new purpose and the lawful basis for processing the data and will notify employees.

**1.2 FAIR PROCESSING OF DATA****1.2.1 Fair Processing Principles**

In processing employees' data the following principles will be adhered to. Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes;
- Relevant to specific purposes and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the specified purposes; and
- Kept securely.

1.2.2 Lawful Processing of Personal Data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, the Firm will use personal information in the following circumstances:

- when it is needed to perform employees' contracts of employment;
- when it is needed to comply with a legal obligation; or
- when it is necessary for the Firm's legitimate interests (or those of a third party) and employees' interests and fundamental rights do not override those interests.

The Firm may also use personal information in the following situations, which are likely to be rare:

- when it is necessary to protect employees' interests (or someone else's interests); or
- when it is necessary in the public interest.

1.2.3 Lawful Processing of Sensitive Personal Data

The Firm may process special categories of personal information in the following circumstances:

- In limited circumstances, with explicit written consent;
- in order to meet legal obligations;
- when it is needed in the public interest, such as for equal opportunities monitoring or in relation to the Firm's occupational pension scheme; or
- when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, the Firm may process this type of information where it is needed in relation to legal claims or where it is needed to protect an employee's interests (or someone else's interests) and the employee is not capable of giving consent, or where an employee has already made the information public. The Firm may use particularly sensitive personal information in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leaves, may be used to comply with employment and other laws;

**DATA PROTECTION POLICY**

- information about employees' physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;
- information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting; and
- information about trade union membership may be used to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

1.2.4 Lawful Processing of Information about Criminal Convictions

The Firm does not envisage that it will hold information about criminal convictions. If it becomes necessary to do so, the Firm will only use this information where it has a legal basis for processing the information. This will usually be where such processing is necessary to carry out the Firm's obligations. Less commonly, the Firm may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect an employee's interests (or someone else's interests) and the employee is not capable of giving consent, or where the employee has already made the information public.

The Firm will only collect information about criminal convictions if it is appropriate given the nature of the role and where it is legally able to do so.

1.3 CONSENT TO DATA PROCESSING

The Firm does not require consent from employees to process most types of employee data. In addition, the Firm will not usually need consent to use special categories of personal information in order to carry out legal obligations or exercise specific rights in the field of employment law. If an employee fails to provide certain information when requested, the Firm may not be able to perform the contract entered into with the employee (such as paying the employee or providing a benefit). The Firm may also be prevented from complying with legal obligations (such as to ensure the health and safety of employees).

In limited circumstances, for example, if a medical report is sought for the purposes of managing sickness absence, employees may be asked for written consent to process sensitive data. In those circumstances, employees will be provided with full details of the information that sought and the reason it is needed, so that employees can carefully consider whether to consent. It is not a condition of employees' contracts that employees agree to any request for consent.

Where employees have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. Once the Firm has received notification of withdrawal of consent it will no longer process information for the purpose or purposes originally agreed to, unless it has another legitimate basis for doing so in law.

1.4 COLLECTION AND RETENTION OF DATA**1.4.1 Collection of Data**

The Firm will collect personal information about employees through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider.

**DATA PROTECTION POLICY**

The table of employee data held within the Firm relates to information which is collected at the outset of employment. From time to time, the Firm may collect additional personal information in the course of job-related activities throughout the period of employment. If the Firm requires to obtain additional personal information, this policy will be updated or employees will receive a separate privacy notice setting out the purpose and lawful basis for processing the data.

1.4.2 Retention of Data

The Firm will only retain employees' personal information for as long as necessary to fulfil the purposes it was collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of personal information are set out in the table of employee data appended to this policy.

When determining the appropriate retention period for personal data, the Firm will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which the personal data is processed, whether the Firm can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances, the Firm may anonymise personal information so that it can no longer be associated with individual employees, in which case the Firm may use such information without further notice to employees. After the data retention period has expired, the Firm will securely destroy employees' personal information.

1.5 DATA SECURITY AND SHARING**1.5.1 Data Security**

The Firm has put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Details of these measures are available upon request. Access to personal information is limited to those employees, agents, contractors and other third parties who have a business need to know. They will only process personal information on the Firm's instructions and are subject to a duty of confidentiality. The Firm expects employees handling personal data to take steps to safeguard personal data of employees (or any other individual) in line with this policy.

1.5.2 Data Sharing

The Firm requires third parties to respect the security of employee data and to treat it in accordance with the law. The Firm may share personal information with third parties, for example in the context of the possible sale or restructuring of the business. The Firm may also need to share personal information with a regulator or to otherwise comply with the law.

The Firm may also share employee data with third-party service providers where it is necessary to administer the working relationship with employees or where the Firm has a legitimate interest in doing so. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services.

**1.6 EMPLOYEE RIGHTS AND OBLIGATIONS****1.6.1 Accuracy of Data**

The Firm will conduct regular reviews of the information held by it to ensure the relevancy of the information it holds. Employees are under a duty to inform the Firm of any changes to their current circumstances. Where an employee has concerns regarding the accuracy of personal data held by the Firm, the employee should contact the Group HR Manager to request an amendment to the data.

1.6.2 Employee Rights

Under certain circumstances, employees have the right to:

- Request access to personal information (commonly known as a “data subject access request”).
- Request erasure of personal information.
- Object to processing of personal information where the Firm is relying on a legitimate interest (or those of a third party) to lawfully process it.
- Request the restriction of processing of personal information.
- Request the transfer of personal information to another party.

If an employee wishes to make a request on any of the above grounds, they should contact the Group HR Manager in writing. Please note that, depending on the nature of the request, the Firm may have good grounds for refusing to comply. If that is the case, the employee will be given an explanation by the Firm.

1.7 DATA SUBJECT ACCESS REQUESTS

Employees will not normally have to pay a fee to access personal information (or to exercise any of the other rights). However, the Firm may charge a reasonable fee if the request for access is clearly unfounded or excessive. Alternatively, the Firm may refuse to comply with the request in such circumstances.

The Firm may need to request specific information from the employee to help confirm their identity and ensure the right to access the information (or to exercise any of the other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

1.8 COMPLIANCE WITH THIS POLICY**1.8.1 The Firm’s Responsibility for Compliance**

The Group HR Manager is tasked with overseeing compliance with this policy. If employees have any questions about this policy or how the Firm handles personal information, they should contact the Group HR Manager. Employees have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues.

1.8.2 Data Security Breaches

The Firm has put in place procedures to deal with any data security breach and will notify employees and any applicable regulator of a suspected breach where legally required to do so. Details of these measures are available upon request.

**DATA PROTECTION POLICY**

In certain circumstances, the Firm will be required to notify regulators of a data security breach within 72 hours of the breach. Therefore, if an employee becomes aware of a data security breach it is imperative that they report it to the Group HR Manager immediately.

1.8.3 Privacy by Design

The Firm will have regard to the principles of this policy and relevant legislation when designing or implementing new systems or processes (known as “privacy by design”).

1.8.4 Employees’ Responsibility for Compliance

All employees, particularly those tasked with regularly handling personal data of colleagues or third parties, have responsibility for ensuring that processing meets the standards set out in this policy. Employees should observe, as a minimum, the following rules:

- Employees must observe to the letter any instruction or guidelines issued by the Firm in relation to data protection.
- Employees should not disclose personal data about the Firm, colleague or third parties unless that disclosure is fair and lawful, in line with this policy;
- Employees must take confidentiality and security seriously, whether the employee considers the information to be sensitive or not.
- Any personal data collected or recorded manually which is to be inputted to an electronic system should be inputted accurately and without delay.
- Employees must not make any oral or written reference to personal data held by the Firm about any individual except to employees of the Firm who need the information for their work or an authorised recipient.
- Great care should be taken to establish the identity of any person asking for personal information and to make sure that the person is entitled to receive the information.
- If an employee is asked by an unauthorised individual to provide details of personal information held by the Firm the employee should ask the individual to put their request in writing and send it to the Group HR Manager. If the request is in writing the employee should pass it immediately to the Group HR Manager.
- Employees must not use personal information for any purpose other than their work for the Firm.
- If an employee is in doubt about any matter to do with data protection they must refer the matter to the Group HR Manager immediately.
- Passwords should not be disclosed and should be changed regularly;
- Employee or third party personal data should not be left unsecured or unattended, e.g. on public transport;
- Unauthorised use of computer equipment issued by the Firm is not permitted;
- Employees must follow the Firm’s “clear desk” policy and ensure that all confidential information, whether containing employee or third party personal data or not, is secured when it is not in use or when the employee is not at work;
- Employees may use only Firm equipment to carry out work and must ensure that devices are password protected and locked when not in use;



DATA PROTECTION POLICY

- As far as possible, employee or third party personal data contained in emails and attachments should be anonymised before it is sent by email; and
- Documents containing sensitive information should be password protected and, if the document requires to be transmitted, the document and password should be transmitted separately.

Any breach of the above rules will be taken seriously and, depending on the severity of the matter, may constitute gross misconduct which could lead to summary termination of employment.