Staff Privacy Notice

Premier Miton Investors ("Premier Miton") is committed to safeguarding the privacy and security of the personal information of our prospective, current and former staff members and our contractors. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Premier Asset Management Limited is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. Under the UK GDPR, we are required to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time. It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

How we use personal information

Most commonly, we use your personal information to manage, oversee and administer all aspects of the employment relationship, including, but not limited to, the recruitment process, payroll, benefits, corporate travel and other reimbursable expenses, training and development, absence monitoring, fitness to work, appraisals, review of conduct and in particular non-financial misconduct, disciplinary and grievance processes, dealing with legal disputes and other administrative, management and human resource related processes.

We may also use personal information about you:

- to comply with our legal obligations (including health and safety) and regulatory duties (including to the Financial Conduct Authority).
- where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests
- in the (probably rare) event that we need to protect your interests or someone else's interests or where it is needed in the public interest;
- in order to comply with our interpretation of regulatory obligations, such as to monitor our staff in respect of non- financial misconduct
- in order to screen for the use of artificial intelligence (AI) generated responses in any initial or subsequent job application with us. (The use of AI may be taken into account in the evaluation of your application).

The types of personal information we process

Personal information refers to information that may, in itself or in combination with other information, be capable of identifying you as an individual. There are "special categories" of more sensitive personal data which require a higher level of protection. The types of personal information that we process include:

- name, gender, home address, telephone number, date of birth, marital status, emergency contacts, salary information, bank and tax information, sick pay, pensions, insurance and other benefits information.
- residency and work permit status, nationality and passport information.
- date of hire, promotions(s), date and details of resignation/termination, work and educational history, professional certifications and registrations.
- leave records, performance appraisals, disciplinary and grievance investigations.
- information required to comply with applicable regulatory requirements, requests from law enforcement authorities or court orders.
- voicemails, emails, correspondence and other work communications created, stored or transmitted by a staff member using Premier's computer or communications equipment; and
- more sensitive personal information such as information about your health, any disabilities , racial or ethnic origin, sexual orientation, criminal convictions or offences, or trade union membership (but we need to have further justification for collecting storing and using this information and we have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

Premier Miton also collects data about the behaviour of its employees to assist in its assessment of their conduct in order to meet regulatory and internal expectations on conduct and culture and to identify any concerns which should be addressed or reported to the FCA. The conduct framework below outlines the conduct metrics that are considered, which include PA dealing breaches, late completion of training and attestations, breaches of the Gifts and Entertainment policy and breaches regarding operational incident reporting. Some of the data points are quantitative and others are qualitative, being subjective and requiring more consideration.

The employee data is collected and compiled bi-annually by the Chief Legal and Compliance Officer and Chief Operating Officer and shared with the Head of HR and CEO for review. Employees who have a significant number of breaches are flagged as requiring review and their conduct may be discussed with their line manager to determine the appropriate course of action, which may be an informal discussion, or as part of their appraisal or through a more formal process, depending on the breach.

At year-end, the full years conduct MI will be considered, and a report produced for the Remuneration Committee to determine whether there should be any consequential impact in

respect of compensation decisions. Any required adjustments will be discretionary, based on individual circumstances.

	Data point
PA Dealing	• Breach of PA Dealing Policy • Late provision of contract notes
Training / Policy Attestations	• Late completion • Failure to pass examination element
Gifts & Entertainment	• Breach of G&E framework
Outside Interests not Disclosed	• Late disclosure • Failure to disclose (and seek approval, where appropriate) on a timely basis
Market Abuse / Mandate Compliance	• Active errors on part of PM or Dealing team
Operational Incident Reporting (Sonar)	• Incidents not reported • Failure to report on a timely basis • Repeated errors
Phishing test / security failures	• Failing clicking test
Procedural / behavioural	• Incidents or breach of procedures (dealing IM, AML, Data Protection etc.)
Acting on monitoring / audit findings	• Not completing audit and CMO findings on time

How we collect your personal information

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of your performance of job related activities throughout the period that you work for us.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Situations in which we will use your personal information

We need all the personal information primarily in connection with our performance of the potential contract (during recruitment) or the employment contract we have entered into with you, or where we need to comply with a legal obligation, or where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

- We may make personal information available to regulatory authorities, potential or future employers, governmental organisations, potential purchasers of Premier Miton businesses, and third parties if required by any regulatory or legal authority.

- When we outsource the processing of your personal information to third parties or provide your personal information to third party service providers, we oblige those third parties to protect your personal information with appropriate security measures and treat it in accordance with law and prohibit them from using your personal information for their own purposes or from disclosing your personal information to others.

- We reserve the right to disclose any personal information we have concerning you if we are compelled to do so by a court of law, where requested to do so by a governmental entity or if we determine it is necessary or desirable to comply with the law, to protect or defend our rights or property, or to protect your interests, some else's or the public interest.

Special categories of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information and we will do so in accordance with our Special Category Data and Criminal Convictions Data Policy. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent (e.g., health consultation or completion of Equality, Diversion and Inclusion surveys.);
- Where we need to carry out our legal obligations and in line with our data security policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our data security policy; or
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards;
- As part of pre-employment screening for all employees, and on-going screening for certain employees by conducting credit and criminal record checks.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

In general, we will not process special category data about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions there may be other reasons for processing, such as if it is in the public interest to do so. The situations where we will use your particularly sensitive personal information are set out below:

- We will use information relating to leave of absence, which may include sickness absence or family related leave, to comply with employment and other laws.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

- We may use information relating to criminal convictions only where it is appropriate given the nature of the role and the law allows us to do so. This will usually be where such processing is necessary to carry out our legal or regulatory obligations and provided we do so in accordance with our Special Category Data and Criminal Convictions Data Policy.

- We may retain copies of documentation which you may have provided during the application process (in which you may have provided special category data).

Security of your personal information

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or use, loss, alteration, or disclosure we have put in place appropriate physical, electronic and operational procedures and security measures intended to safeguard and secure the information we collect. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a legitimate business need to know and will only process your information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

All Premier Miton staff have a legal duty to keep information confidential and access to confidential information is restricted only to those who need it.

Retention of your Personal Information

We will only retain your personal data for as long is necessary for the purpose for which it was collected and delete / destroy data in line with our data retention policy. When a staff member leaves Premier Miton, personal data that is no longer required is deleted (for example, next of kin details, bank account details, contact details, etc.). In relation to job applications, all personal data is deleted 12 months after the recruitment process has been completed.

We retain anonymised statistical information to help inform our recruitment activities.

Data sharing

We will share your data with other entities, where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

The following activities are carried out by third-party service providers: payroll, pension administration, employee share scheme and some benefits provision and administration.

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Your rights in connection with personal information

Under the UK GDPR, in certain circumstances, you have the right to:

- Request access confirmation that your data is being processed, access to your personal data, etc. We will provide information in response to a subject access request in accordance with the relevant legislation (please see the Data Security Policy for more details).
- Request correction the right to have personal data corrected if it is inaccurate or incomplete.
- Request erasure (to be forgotten) – the right to request the deletion or removal of personal data where there is no compelling reason for us to continue to process it.
- Object to processing this enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the transfer of personal data – this allows individuals to retain and re-use their personal data for their own purposes across difference services.

Please keep us updated if your personal information changes during your working relationship

with us.

Access to your personal information

Under the UK GDPR, you have a right to request a copy of any personal information Premier Asset Management Limited holds about you.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your 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

Please refer to the Data Security Policy or contact our Data Protection Officer for more information.

How to contact us

Premier Asset Management Limited is the data controller. Our Data Protection Officer can be contacted at 1 Eastgate Court, High Street, Guildford, Surrey, GU1 3DE or dataprotection@premiermiton.com or 01483 30 60 90.