KI

Risk, simplified.

Privacy Notice for Directors, employees, workers and contractors

Introduction

We're committed to protecting the privacy and security of your personal data. When we talk about "personal data", as the context requires, this will include "special categories of personal data", which involves more sensitive information about you.

This privacy notice describes how we are or will be processing personal data about you in order for you to work here, while you work here and afterwards if you leave. "Processing" covers things like collecting, using, storing, disclosing, erasing or destroying your personal data.

This applies to all Directors, employees, workers and contractors. It's not part of your contract of employment or other contract to provide services.

This Privacy Notice applies to Ki Financial Limited and its group companies ('Ki'), including Ki Group Services Limited, among others.

Identity and contact details of the data controller and the data protection officer

Ki is a "data controller". This means we're responsible for deciding how we process personal data about you.

The contact details of Ki are:

The Leadenhall Building
122 Leadenhall Street
London
EC3V 4AB

The principal contact for data protection at Ki is our Compliance Lead:

Andy Mills, Compliance Lead / andy.mills@ki-insurance.com

The Compliance Lead is responsible for overseeing compliance with this privacy notice and for handling any data protection queries or issues involving Ki.

What type of personal data do we process about you?

We may process the following categories of personal data about you:

- If you require a visa to work at Ki, we or our appointed representatives may be legally required to obtain certain information about you. We'll inform you about this separately.
- Copies of right-to-work verification details (such as passport details) that you share with us.
- Other recruitment information, including third party references and other information on your CV or your cover sheet.
- Previous employment history, including education background information.
- Personal contact details such as name, title, address, telephone numbers, and personal email address.
- Your date of birth, gender, marital status and details of dependants.
- Next of kin and emergency contact information.
- Your National Insurance number.
- Your bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Copy of your driving licence.
- Current employment records (including job titles, work history, working hours, place of work, start date, training records, qualifications, professional memberships and professional body membership numbers).
- History of pay, bonus, LTIP information, student loan information, other benefits (and US only: benefit election information).

- Details of performance and Performance Reviews.
- Where applicable, disciplinary and grievance information.
- CCTV footage and other information obtained electronically, like swipecard records.
- Information about your use of our information and communications systems.
- Photographs.
- Reason for leaving and confidential references provided by us, as well as information required to provide reference information.
- Details of any payments made on termination.

We may also process the following "special categories" of more sensitive personal data:

- Information about your race or ethnicity, religious beliefs, sexual orientation.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences– please see "Information about criminal convictions" below for further information
- Information about political party membership or political affiliations.
- Information about your trade union membership or that of a companion at a disciplinary/grievance meeting.

How do we collect your personal data?

We typically collect personal data about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency. We sometimes collect additional information from third parties including former employers (in the form of references). There are lots of forms that you might complete while you work here, where you provide personal data – these forms are collected and processed by the HR team.

We'll collect additional personal data in the course of job-related activities while you work for us. For example, if you complete an Equality and Diversity Monitoring form on the Pre-boarder portal, this will reveal information about your race or ethnicity, whether you consider yourself to be disabled, your sexual orientation, religion and belief, and gender monitoring.

What are the legal bases and the reasons why we process your personal data?

We'll only use your personal data as permitted by law. We'll typically use your personal data in any of the following circumstances:

1. Where we have your consent to do so.
2. Where we need to perform the contract we have entered into with you.
3. Where we need to comply with a legal obligation.
4. Where the processing is necessary to perform a task in the public interest.
5. Where it's necessary for our legitimate interests (or those of a third party) but where your interests and fundamental rights don't override those interests. We're required to specify what the legitimate interests are (see below for more details).

The examples given below aren't an exhaustive list of purposes for processing your personal data, and we have the right to add to them at any time.

Consent

If you work in the underwriting and claims teams, you have the option of having your photograph and contact details uploaded on to the Ki App so you can be contacted by brokers. Anyone with access can see your availability from the app. This is entirely voluntary and you can withdraw your consent at any time.

Necessary for the performance of a contract with you

The following purposes come under this category:

- Making sure you're paid and that you have the correct tax, NICs and any other appropriate deductions (season ticket loans, student loans etc) from any payments.
- Management and planning, including accounting and auditing.
- Administering your contract (eg by reviewing your working hours to check holiday and rest break entitlement, checking your start date for eligibility for age–related benefits).
- Making decisions about salary and other payment reviews.
- Assessing your suitability for the role, including decisions about promotions or other role changes.
- Where applicable, providing you with benefits including holiday, pension (including liaising with your pension provider/administrator), private medical insurance (for yourself and/or family members, as applicable), life assurance and season ticket loans, where such benefits are part of your contract.
- Making sure (as far as possible) that your wishes are fulfilled regarding death–in–service payments and that your next of kin are contacted in the event of an emergency (hence the need for third party information, usually comprising details of partners and/or dependants).
- Letting you apply for flexible working or other family rights like maternity, paternity, parental leave etc – this requires details of your partner/dependants.

Necessary to comply with a legal obligation

- Checking you're legally entitled to work in the UK. Your nationality, immigration status and information from related documents, like your passport and other ID such as driving licence and immigration documents.
- Handling any legal disputes involving you or third parties, including accidents at work.
- To prevent fraud.

Necessary for our legitimate interests or those of a third party

Compensation and Benefits:

- Provision of benefits that may not be deemed to be contractual, such as LTIP awards.
- US only: benefit election, Flexible Savings Account, 401k beneficiary.
- The legitimate interest is to ensure you receive and we administer benefits which are not necessary for the performance of your contract.

Learning and Development:

- Personal data provided by you on training forms, book request forms, graduate forms, conference application forms, high performance forms, various study and exam booking forms, supplier forms (including various CII forms) – the legitimate interest is to make sure your learning and development needs are addressed and documented.

Recruitment:

- Personal data provided by you on new starter forms or temporary new starter forms, specifically your gender, mobile phone number, next of kin details – the legitimate interests are: for identity and reporting, for emergency contact/disaster recovery.
- Personal data provided by you on your CV and cover sheet – the legitimate interests are: to ascertain your suitability for employment/engagement.

HR Operations:

- Personal data obtained through our external background screening (which may include address history, employment history, education background, criminal records information (see below for more details), credit history and regulatory references under the Senior Managers and Certification Regime) – the legitimate interests are: for verifying the information on your CV, to verify the relevant

qualifications/requirements for the role, to verify your employee declaration and as necessary for compliance and as required by regulatory bodies, and to ensure that there are no issues with your credit history that could place unnecessary risks on Ki or third parties.

- Personal data obtained about grievance and disciplinary issues – the legitimate interest is to address issues and concerns from either side in the employment relationship.
- Personal data from Performance Reviews – the legitimate interest is to make sure your performance is assessed and documented. This is so we can track any improvements we need to work on, or to reward performance.
- Personal data from monitoring our IT systems – the legitimate interest is to make sure compliance with our IT policies and the integrity of our IT systems, network and information security. This includes preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Personal data obtained through CCTV – the legitimate interest is the protection of health and safety (including the identification of individuals on premises in the event of a fire or other serious incident) and the prevention and detection of criminal acts.
- Personal data obtained through swipecard technology – the legitimate interest is to make sure only authorised members of staff or authorised visitors are on site. This lets us safeguard systems and property from unauthorised access, destruction or theft. We might also use this to provide evidence about any issues regarding timekeeping and attendance.
- We may sometimes obtain personal data when filming in the office for executive presentations, filming of staff for use in inductions, or other internal events. We'll tell you in advance if you're in the vicinity of the filming, so you have the chance to not be filmed. We'll store media on the Hub, so it can't be seen externally. The legitimate interest is to provide internal updates to Ki through interactive media, improve staff engagement and improve our induction processes.
- Reference information – we usually only provide basic factual information about ex-employees – or departing employees – to prospective new employers. However, if we have legitimate concerns which, if not disclosed to a prospective new employer, could mean we breach our duty of care to that prospective new employer, we'll disclose as we reasonably consider necessary to satisfy that duty.

If you fail to provide personal data

If you fail to provide certain information when asked, and we can't get it from a third party or publicly available source, 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 might not be able to comply with our legal obligations (such as to ensure the health and safety of our workers). Depending on the nature and importance of the information requested, we may either have to stop employing you or engaging you or withdraw an offer of employment or engagement.

How we use special categories of personal data

"Special categories" of personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data. We may process special categories of personal data in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our data protection policy and related policies (such as managing sickness absence, complying with health and safety obligations).
3. Where it's needed in the public interest, such as for equal opportunities monitoring (where such information is provided by you).
4. Where we need it to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

We may process this type of information for legal claims or where it's needed to protect your interests (or someone else's interests) and you're not capable of giving your consent. Or, where you've already made the information public.

We'll use your special categories of personal data in the following ways:

- We'll use information relating to leaves of absence, which may include sickness absence or family-related leaves, to comply with employment and other laws.
- We'll use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace, and the health and safety of others. We'll also assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits. We may obtain information about your physical and mental health from medical and occupational health professionals that we engage, and from our insurance benefit administrators.
- We'll use information about your race or national or ethnic origin, religious or other beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Information about criminal convictions

We may only use information about criminal convictions where the law allows us, and we have a legitimate reason, to do so. For some roles there's a regulatory requirement or expectation that criminal record checks will happen. For all roles we'll do appropriate checks to protect our business and systems, and to make sure we maintain the trust of clients. Our legitimate interests are to make sure that, where practical, we have trustworthy staff we can rely on to work within the law. The checks are necessary to let us perform or exercise our employment law rights and obligations. In all cases we'll ask you to authorise our third party screening provider to obtain a basic criminal record disclosure from the Disclosure and Barring Service (DBS) as part of our background screening checks. For most roles within Ki, any criminal record disclosures will not include information on spent convictions. In instances where they are, we'll tell you separately in advance of the checks.

We may also use information about criminal convictions where it's necessary for legal claims. We'll also use it where necessary to protect your interests (or someone else's interests) and you're not capable of giving your consent, or where you have already made the information public. If you'd like more details about this then please ask.

Who might we share your personal data?

We may have to share your data with third parties, including third party service providers and any sub-contractors of those service providers. See below for further details.

We require third parties to respect the security of your data and to treat it in accordance with the law.

If we need to transfer your personal data outside the EU, we'll make sure it's done on a lawful basis. For instance, information about your involvement in the Employee Share Ownership Plan will need to be transferred to Fairfax Financial Holdings Limited, based in Canada. Canada is deemed by the European Commission to be a destination with adequate data protection laws, so you can expect a similar degree of protection for your personal data. For other countries we'll make sure there are appropriate safeguards in place to protect your rights and interests. Furthermore, if your work requires you to communicate with third parties (for example clients) outside of the EU, your personal data will be transferred by you through any information you provide in such communications.

Why might we share your personal data with third parties?

We may share your personal data with third parties where required by law, where it's necessary to administer the working relationship with you or where we have another legitimate interest in doing so. We've given some examples above where disclosure will be appropriate or necessary.

Which third party service providers process my personal data?

"Third-parties" includes third party service providers (including contractors and sub-contractors), such as pension provider, benefit providers (life assurance, private medical insurance provider), payroll providers, public authorities, legal advisors, occupational health and welfare providers, outplacement services, training providers and professional bodies.

How secure is your information with third party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal data in line with our policies. We don't let our third-party service providers use your personal

data for their own purposes unless they're data controllers in their own right in relation to your personal data. Where they operate as our "data processors" (i.e. they process your personal data on our behalf and acting only on our instructions), we only let them process your personal data for specified purposes and in accordance with our instructions.

What about disclosure to other third parties?

We may share your personal data with other third parties, for example in the possible sale or restructuring of Ki. We may also need to share your personal data with a regulator, to external legal or other professional advisers, or to otherwise comply with the law.

How long will we retain your personal data?

We'll only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal data are in our Document Retention and Secure Document Disposal Policy.

In some circumstances we may anonymise your personal data so it can't be associated with you, in which case we may use such information without further notice to you. Once you're no longer an employee, worker or contractor of the company we'll retain and securely destroy your personal data in accordance with our Document Retention and Secure Document Disposal Policy.

What are your rights and obligations as a data subject?

Your duty to inform us of changes

It's important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes while you're working with us.

Your rights in connection with personal data

Under certain circumstances, by law you have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). You'll get a copy of the personal data we hold about you and you can check we're lawfully processing it.
- Request correction of your personal data. This lets you correct any incomplete or inaccurate information we hold about you.
- Request erasure of your personal data. You can ask us to delete or remove personal data, but only where there's no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you've exercised your right to object to processing (see below).
- Object to processing of your personal data where we're relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- Request the restriction of processing of your personal data. You can ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal data to another party.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact the Compliance Lead in writing.

No fee usually required

You won't have to pay a fee to access your personal data (or to exercise any of the other rights).
However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse the request in such circumstances.

What we may need from 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 make sure personal data isn't disclosed to anyone who has no right to receive it.

What are your rights to withdraw consent to processing?

You may withdraw your consent to allow us to continue processing your personal data, but only where consent was sought as a lawful means of processing your personal data.

In the limited circumstances where you may have provided your consent to the processing of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Compliance Lead. Once we've received notification that you've withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

What are your rights to lodge a complaint about the way your personal data is being processed?

Firstly we would urge you to contact the Compliance Lead in writing. If you're not satisfied with the Compliance Lead's response, you can contact the Information Commissioner's Office ("ICO") on 0303 113 1113.

You're free to contact the ICO at any time. However, the Compliance Lead may be able to help more quickly.

Personal data received from someone other than you

If we obtain personal data from someone other than you (such as a referee, or information from a regulator), we'll provide you with information as to the source of such personal data and, if applicable, whether it came from publicly available sources.

What data security measures are in place to protect my personal data?

We have put in place measures to protect the security of your information – you can ask for the details. There are digital employee files held securely on our internal IT systems which can only be accessed by the HR team. You can also read the Ki Corporate Information Security Policy which sets out the information security framework we use. See also the Ki Data Classification Policy and the accompanying Data Classification FAQs, on the Hub, which set out details of the encryption methods that should be applied according to the class of data that is being sent electronically. You can also look at the flow diagram "Where should you store your data?" for details of where data should be stored, according to its data classification. This will apply to your personal data as well as personal data of third parties.

Third party data processors will only process your personal data on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

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.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we'll let you know if we do, with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

If you have any questions about this privacy notice, please contact the Compliance Lead.