

# Employee Privacy Notice

## What this Notice covers

The Company is committed to protecting the privacy and security of your personal information.

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 General Data Protection Regulation (GDPR) and data protection legislation.

It applies to all current and former employees, workers and contractors.

## Identity of the data controller

Interr Limited is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation 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.

## Categories of personal data we process

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, personal email addresses; date of birth; marital status and certificates; gender and dependants
- Next of kin and emergency contact information
- National Insurance number
- SIA licence
- Disclosure and Disclosure information
- Proof of address
- Bank account details, payroll records and tax status information and HMRC information
- Information about criminal convictions and offences, including credit checks and country court judgements
- Previous work or education history within last 5 or 10 years
- Previous addresses within last 5 or 10 years
- All vetting related information, paperwork and files in accordance with BS7858:2019
- Travelling details if required for vetting under BS7858:2019
- Salary, annual leave, pension and benefits information
- Start date
- Leaving date and leaving documentation
- Copy of driving licence
- Reference / confirmation of employment letters
- Recruitment information (including copies of right to work documentation, all stages of interview process and paperwork related to them as well as induction assessments, references and other information included in a CV or cover letter or as part of the application process)
- Employment records (including terms and conditions of employment, job description and code of conduct, work history, working hours, training records, promotions or change of terms and conditions and professional memberships)
- Compensation history
- Performance information including appraisals and performance improvement plans

- Details of any records of conversations, investigations, disciplinary and grievance proceedings you have been involved in
- Details of any leave you have taken including holidays; sickness; family and parental leave.
- CCTV footage
- Information obtained through electronic means such as swipecard records and biometric means of identification
- Information about your use of our information and communications systems
- Photographs
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Information about your health, including any medical condition, health and sickness records and details of any disability for which we may need to make reasonable adjustments
- Genetic information and biometric data

## Sources of personal data

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

We also collect additional personal information in the course of job-related activities throughout the period you are working for us.

## Our lawful bases for processing your data

We will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.
- 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.

## Our purposes for processing your data

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Paying you and, if you are an employee, deducting tax and National Insurance contributions
- Liaising with your pension provider
- Administering the contract we have entered into with you
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with possible legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud

- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- Equal opportunities monitoring
- For completion of vetting under BS7858:2019

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information

We will not use your data for any purpose other than the recruitment exercise for which you have applied. If your application is unsuccessful, and we would like to keep your personal data on file in case there are future employment opportunities for which you may be suited, we shall ask for your consent before we keep your data for this purpose and you are free to withdraw your consent at any time.

## Who has access to your data

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

We will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. We may share then your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, meet our obligations under staff contracts or where we have another legitimate interest in doing so.

Recipients of your data may include former employers to obtain references for you, employment background check providers to obtain necessary background checks and for certain roles, the Disclosure and barring Service to obtain necessary criminal records checks.

Recipients of your data may also include third-party service providers (such as payroll and pensions providers, vetting company, government bodies, company auditors); other related business entities; a regulator or to otherwise comply with the law.

Where we do so, we will require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

## Security of your data

The Company is required to implement and maintain appropriate safeguards to protect sensitive and personal data, taking into account in particular the risks to data subjects presented by unauthorised or unlawful processing or accidental loss, destruction of, or damage to the sensitive or personal data. Safeguarding will include the use of encryption or pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorised to use personal data have access to it), integrity and availability of the personal data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

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.

## How we decide how long to retain your data

We will only retain your personal information 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.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

## Your rights

Under GDPR, individuals have a range of rights. These include knowing how their data is being collected and used, requesting access to data held about them and having data erased or corrected.

- **To be informed** - An individual's right to be informed is via this privacy notice.
- **Of access** – Any requests must be submitted via a subject access request (SAR) and companies comply within 30 days.
- **To rectification** – To have inaccurate or incomplete data rectified – known as the right to rectification.
- **To erasure** - An individual can request the deletion or removal of personal data. Not all requests for erasure must be complied with. Requests can be denied if the data is in the public interest, or it is required to comply with a legal obligation.
- **To restrict processing** – An individual can contest the accuracy of their information so they can ask the Company to restrict processing until accuracy is verified.
- **To data portability** - Give individuals more choice so they don't feel compelled to stay with a particular service due to the effort involved in moving.
- **To object** - the right to object to the processing of their personal data in certain circumstances, requested in writing with specific reason, however the Company can refuse if we can demonstrate completing legitimate grounds for processing.
- **To automated decision making and profiling** - Profiling is any form of automated processing used to evaluate, analyse or predict personal aspects of an individual, e.g., performance at work, economic situation. An individual has the right not to be subject to a decision based solely on automated processing if it significantly affects them.

If you believe the Company has not complied with your rights, you can complain to the Information Commissioner.

## What if you do not provide personal data?

If you do not provide personal data, it is likely to be impossible for the Interr Limited to enter into, or to continue with, an employment relationship with you.

## Automated decision-making

The Company may make use of electronic automated decision-making systems. we would only do so in the following circumstances:

- where we have notified you of the decision and given you 21 days to request reconsideration.
- where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- in limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

Employment decisions are not based solely on automated decision-making.

## Changes to this Privacy Notice

The Company reserves the right to update this privacy notice at any time, and we will provide you 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 information.

## Policy Review

This policy may be amended by Interr at any time in order to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.



Mick Tabori - CEO  
January 2024