Data Protection Policy

Introduction

This policy applies to employees, workers, contractors and relevant parties. This policy details your rights and obligations in relation to your personal data and the personal data of third parties that you may come into contact with during the course of your engagement with Interr. Ensuring that all data is secure and properly dealt with is of paramount importance to Interr, and we have this policy in place ensure we conform fully with General Data Protection Regulations (GDPR) and other relevant Data Protection legislation.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal and sensitive data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Interr Ltd is registered with the Information Commissioner's Office. Details of the Company registration are published on the Information Commissioner's website.

Interr shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the GDPR (2018) and DPA (2018):

"Personal data" is any information that relates to a living individual who can be identified from that information.

"Processing" is any use that is made of personal data, including collecting, storing, amending, disclosing or destroying it.

"Controlling" is determination of the purposes for which and the manner in which any personal data are, or are to be, processed.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or political beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

In the course of your work you may come into contact with or use personal data about employees, clients, customers and suppliers, for example their names and home addresses. If you have access to any of the personal, special categories or criminal records data of staff or of third parties, you must comply with this Policy. Failure to comply with the Policy and procedures may result in disciplinary action up to and including dismissal without notice.

Why this policy exists

This Data Protection policy ensures Interr Ltd:

- Complies with Data protection law and follows good practise
- Protects the rights of staff, customers and partners
- Is open about how its stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Risks

This policy helps protect the Company from some very real data security risks, including:

- *Breaches of confidentiality* – information being given out inappropriately
- *Failing to offer choice* – All individuals should be free to choose how the company uses data relating to them
- *Reputational damage* – the company could suffer if hackers successfully gained access to sensitive data

Data Protection principles:

The Company processes all sensitive data in accordance with the following data protection principles:

- the Company processes personal data lawfully, fairly and in a transparent manner;
- the Company collects personal data only for specified, explicit and legitimate purposes;
- the Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of the processing;
- the Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- the Company retains personal data only for the period necessary for the processing;
- the Company adopts appropriate measures to make sure that personal data is secure and is protected against unauthorised or unlawful processing and from accidental loss, destruction or damage.

Your entitlements

Data protection legislation prescribes the way in which the Company may collect, retain and handle personal data. The Company will comply with the requirements of data protection legislation and all employees and contractors who handle personal data in the course of their work must also comply with it.

The Company will inform individuals of the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data about individuals for other reasons.
Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the rules relating to special categories of data and criminal records data.

The Company will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment or engagement of an employee, worker, contractor, volunteer, or intern is held in the individual's personal file (in hard copy or electronic format, or both), and on HR systems. The Company will normally keep personal data for no longer than six years after an employee has left the Company's employment.
Different categories of data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be securely destroyed. Data relating to unsuccessful job applicants will only be retained for a period of one year and after consent has been obtained from the job applicant to process their personal data.

The periods for which the Company holds HR-related personal data are contained in its privacy notices.

Access to your personal data [subject access requests]

You have the right to make a subject access request. If you wish to access a copy of any personal data being held about you, you must make a written request for this to the Human Resources for attention of the Data Protection Officer. Note that the Company will always check the identity of the employee making the request before processing it.

If you make such a request, the Company will tell you:

- whether or not your data is processed and if so why; the categories of personal data concerned and the source of the data if it is not collected from you;
- to whom your data may be disclosed, including any recipients located outside the European Economic Area (EEA) and the safeguards that apply to any such transfers;
- for how long your personal data is stored or how that period is decided;
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the has failed to comply with your data protection rights; and
- whether or not the Company carries out any automated decision-making and the logic involved in such decision-making.

The Company will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made the request electronically, unless you request otherwise.

If you want additional copies, the Company will charge a fee, which will be based on the administrative cost of providing the additional copies.

Other rights

You have a number of other rights in relation to your personal data. You can require the Company to:

- rectify inaccurate data;
- stop processing or erase data if your interests override the Company legitimate grounds for processing data (where the Company relies on its legitimate interests as a lawful basis for processing data);
- stop processing or erase data if it is unlawful; and
- stop processing data for a period if it is inaccurate or if there is a dispute about whether or not your interests override the Company legitimate interests for processing the data.

If you wish to make a complaint that this policy has not been followed in respect of personal data the Company holds about you, you should raise the matter with the Human Resources Department. If the matter is not resolved, it should be raised as a formal grievance under the Company's grievance procedure.

Your responsibilities and Information Security

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.

You are responsible for helping the Company keep your personal data accurate and up to date. You should let the Company know if personal data provided to the Company changes, for example, if you change bank or move house.

You may have access to the personal data of other individuals and of our customers or clients in the course of your employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the Company relies on you to help meet its data protection obligations and information security protection .

- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- If you receive a request for personal information about another employee, you should forward this to the Human Resources department, who will be responsible for dealing with such requests.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected.
- Comply with all policies related to Data Protection and Information Security to protect personal, company and client's data.
- Report any potential, suspected or actual information security or data protection breaches.

Compliance with the data protection legislation and Information Security is the responsibility of all employees. Any questions or concerns about the interpretation of this policy should be taken up with the Human Resources Department.

If you have access to personal data, you are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Company) who do not have appropriate authorisation;
- do not give out personal data except to the data subject. In particular, it should not be given to someone, either accidentally or otherwise, from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.

- be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
- to keep data secure (for example by complying with rules on access to premises, computer access including password protection, and secure file storage and destruction);
- not to remove personal data or devices containing or that can be used to access personal data, from the Company premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

You are also responsible for protecting the personal data that you process in the course of your duties. You must therefore handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

You must comply with all procedures, policies and technologies we put in place to maintain the security of all personal and sensitive data from the point of collection to the point of destruction.

You must comply with all applicable aspects of our Information Security Policy, and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Law standards to protect personal and sensitive data.

Failure to observe these requirements may amount to a disciplinary offence which will be dealt with under the Company disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct, could lead to your dismissal without notice and may result in legal action taken against you.

Processing special categories and criminal records data

The Company will process special categories and criminal records data primarily where it is necessary to enable the Company to meet its legal obligations and in particular to ensure adherence to health and safety legislation; vulnerable groups protection legislation; or for equal opportunities monitoring purposes. In some cases, the Company will not process special categories or criminal records data without your consent.

Procedure

The Company keeps a record of its processing activities in respect of sensitive personal data in accordance with the requirements of data protection legislation.
Personal data relating to employees may be collected by the Company for the purposes of:

- recruitment, promotion, training, redeployment and/or career development, such as references, CVs and appraisal documents;
- determining the terms on which you work for us and checking you are legally entitled to work in the UK;
- determining the terms on which you work for us and administering the contract we have entered into with you;
- administration and payment of wages;
- emergency contact details;
- bank/building society details, deducting tax and National Insurance contributions;
- liaising with your pension provider and calculations of pension;
- calculations of certain benefits;
- disciplinary or grievance issues;
- vetting in line with BS7858;
- conducting performance reviews, managing performance and determining performance requirements;
- recording of communication with employees and their representatives;
- compliance with legislation;
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers;

- staffing levels and career planning;
- business management and planning, including accounting and auditing;
- 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 policies;
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- to record digital meetings to allow replay or storage;
- to record cctv video and audio recordings to allow replay or storage;
- to conduct data analytics studies to review and better understand employee retention and attrition rates, and
- equal opportunities monitoring.

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

Sensitive data relating to an external party such as clients or subcontracts may be collected by the Company for the purposes of:

- processing invoices, payments, standing orders or any other payments
- identifying suitable opportunities and action plans
- data analysis, including performance reports to be shared both internally and externally
- understanding internal processes
- preventing fraud and other security related matters

How we use special categories and criminal records data

"Special categories" data and "criminal records" data require higher levels of protection. We need to have further justification for collecting, storing and processing these types of personal data. we may process special categories or criminal records data in the following circumstances:

- in limited circumstances, with your explicit written consent;
- where we need to carry out our legal obligations;
- where it is needed in the public interest, such as for equal opportunities monitoring, or in relation to our occupational pension scheme;
- where it is needed to assess your working capacity on health grounds.

Less commonly, we may process this type of data where it is needed in relation to legal claims or where it is needed to protect your vital interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Accuracy of personal data

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date, employees' personnel files do not contain a backlog of out-of-date or irrelevant information and to check there is a sound business reason requiring information to continue to be held.

To ensure the Company files are accurate and up to date, and so that the Company is able to contact you or, in the case of an emergency, another designated person, you must notify the Human Resources Department as soon as possible of

any change in your personal details (e.g., change of name, address, telephone number, loss of driving licence where relevant, next of kin details, etc).

Security of personal and sensitive data

The Company will ensure that sensitive and personal data is not processed unlawfully, lost or damaged. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Sensitive data or personnel files are confidential and are stored on secure shared drive. Only authorised employees have access to these files. For a list of authorised employees, please contact the Human Resources Department. Files will not be removed from their normal place on the secure shared drive without good reason, all files are stored confidentially by means of password protection, encryption or coding. Only those employees that have been authorised to access personal data will be able to do so. The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.

Sensitive or personal data will not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection relation to the processing of personal data and the following conditions are met:

- the Clients have, or The Company have, provided appropriate safeguards in relation to the transfer;
- the data subject has enforceable rights and effective legal remedies;
- the Company complies with our obligations under the Data Protection Legislation by providing an adequate level of protection to any personal data that is transferred; and
- the Company comply with any reasonable instructions notified to the Company in advance with respect to the processing of the personal data;

If you have access to personal data during the course of your employment, you must also comply with this obligation. If you believe you have lost any personal data in the course of your work, you must report it to your manager immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

Data Masking

The company will also use Data masking, also known as data obfuscation or data anonymization, to protect sensitive information by replacing, encrypting, or scrambling original data with fictitious or pseudonymous data. Data masking aims to ensure that sensitive information remains confidential and compliant with privacy regulations.

Data breaches

The Company will record all data breaches regardless of their effect. If we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about the likely consequences of the breach and the mitigation measures we have taken.

Access to personal data ["subject access requests"]

To make a subject access request, you should send your request to the Company. In some cases, the Company may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require.

We will normally respond to a request within one month from the date we receive it. In some cases, such as where the Company processes large amounts of the individual's data, we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a

request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.

If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the Human Resources Department. You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of data protection legislation. A serious breach of data protection is also a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

This policy does not form part of an employee's contract of employment, but it is a condition of employment that If you have access to the personal, special categories or criminal records data of employees or of third parties, you must comply with this Policy. Therefore, any failure to follow it can result in disciplinary proceedings up to and including dismissal without notice.

Data Disposal

Personal or sensitive data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).
When any sensitive or personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of in line with the rest of the Company policies, such as Policy on the Secure Disposal of IT Equipment and Company held data.

Policy Review

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