Privacy Policy

DEFINITIONS:

GDPR: General Data Protection Regulation which is legislation setting out the legal framework for collection and processing of personal information of individuals.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess 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.

Special Category Data: this is personal data which the GDPR says is more sensitive and so needs more protection. It includes information revealing 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, and Personal Data relating to criminal offences and convictions.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or Company safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or Company that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Processor: Is a person or Company responsible for processing personal data on behalf of the data controller

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Manager: the person with responsibility for data protection compliance.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general employee privacy statements or they may be stand-alone privacy statements covering Processing related to a specific purpose.

Processing or Process: 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. INTRODUCTION

This privacy policy sets out how we handle the Personal Data of our employees, customers, workers, suppliers and other third parties and applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or suppliers.

We recognise that the correct and lawful treatment of Personal Data will maintain confidence and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to large fines for failure to comply with the provisions of the GDPR. Every employee is responsible for complying with this policy.

You must always contact the Data Protection Manager in the following circumstances:

- if you are unsure about the retention period for the Personal Data being processed
- if you believe there has been a Personal Data breach
- if you need any assistance dealing with any rights invoked by a Data Subject
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties

2. PERSONAL DATA PROTECTION PRINCIPLES ARE THAT IT SHOULD BE:-

(a) Processed lawfully, fairly and in a transparent manner {Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation)

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and Company measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred out of UK without appropriate safeguards being in place.

(H) made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

(I) Where relevant you must be able to demonstrate compliance with the data Protection Principles listed above (Accountability).

3. LAWFULNESS, FAIRNESS, TRANSPARENCY

3.1 LAWFULNESS AND FAIRNESS

You may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process Personal Data fairly and without adversely affecting the Data Subject. So you can establish and evidence one of the principles below:

(a) The Data Subject has given their Consent;

(b) The Processing is necessary for the performance of a contract with the Data Subject;

(c) To meet our legal compliance obligations;

(d) To protect the Data Subject's vital interests;

(e) To pursue a legitimate interest, there are three elements to the **'legitimate interests':-**

I) Identify a legitimate interest which can be those of the Company's own interests OR the interests of third parties. They can include commercial interests, individual interests or broader societal benefits

ii) Show that the processing is necessary to achieve it; the processing must be necessary, if the Company can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

iii) Balance it against the individual's interests, rights and freedoms. The Company must balance our interests against the individual's. If the individual would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override our legitimate interests.

Personal Data which has 'Special Category' status;

With this type of data the Company need to evidence one of the grounds set out above together with one other reason as set out below;

(a) Explicit consent
(b) Processing is necessary for the carrying out obligations under employment or social security legislation
(c) Processing is necessary to protect the vital interests of a data subject
(d) Processing is carried out by a not for profit Company and the processing only relates to members of that body
(e) Processing relates to personal data made public by data subject
(f) Processing necessary for the establishment or defence of legal claims
(g) Processing is necessary for the reasons of substantial public interest
(h) Processing is necessary for purposes of preventative or occupational medicine for assessing the working capacity of an employee etc.
(I) Processing is necessary by reason of public interest in the area of Public health

Gaining Consent

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement OR positive action to the Processing. If 'Explicit consent is being relied upon this must be in writing.

Data Subjects are able to easily withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for d different and incompatible purpose which was not disclosed when the Data Subject first consented.

3.2 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

Data Controllers need to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from them or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and Data Protection Manager, how and why we will use, process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

4. PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

5. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only Process Personal Data when performing your job duties requires it.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guideline

6. ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards, you must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

7. STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

At the end of this Policy the Company has set out a retention table indicating the length of time that HR data can be kept for this must be referred to and followed where appropriate.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

8. SECURITY INTEGRITY AND CONFIDENTIALITY

8.1 PROTECTING PERSONAL DATA

The Company must ensure that Personal Data is adequately secured against unauthorised or unlawful Processing, against accidental loss, destruction or damage.

You must follow all procedures we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

8.2 REPORTING A PERSONAL DATA BREACH

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Protection Manager. You should preserve all evidence relating to the potential Personal Data Breach.

9. DATA SUBJECT's RIGHTS AND REQUESTS

Data Subjects have these rights when it comes to how we handle their Personal Data:-

(a) Withdraw Consent to Processing at any time;

(b) Receive certain information about the. Data Controller's Processing activities;

(c) Request access to their Personal Data that we hold;

(d) Prevent our use of their Personal Data for direct marketing purposes;

(e) Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) Restrict Processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(j) Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(I) make a complaint to the supervisory authority; and

(m) In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the data protection manager.

10. RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data Processing activities. You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the data protection manager clear descriptions of the Personal Data types, Data Subject types, processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

11. TRAINING AND AUDIT

We are required to ensure alt staff have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance. You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

12. DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible.

13. SHARING PERSONAL DATA

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. You may only share the Persona! Data we hold with another employee if the recipient has a job-related need to know the information. You may only share the Personal Data we hold with third parties, such as our service providers if:"

(a) They have a need to know the information for the purposes of providing the contracted services;

(b) Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject’s Consent has been obtained;

(c) The third party has agreed has agreed in writing to comply with the required data security standards, policies and procedures and put adequate security measures in place.

RETENTION PERIODS FOR EMPLOYEE DATA

Type of employment record	Format and Location	Retention or Recommendation
Job applications and interview records of unsuccessful candidates	Paper or electronic	6 months after notifying unsuccessful candidates. Or If both agree CV can be held on file
Human resources and training documentation	Paper or electronic	While employment continues and up to six years after employment ceases
Written particulars of employment, any variations. Working time opt out, Privacy Notices	Paper or electronic	While employment continues and up to six years after employment ceases
Annual Leave Records	Paper or electronic	Six years or possibly longer if leave can be carried over year to year
Payroll and Wage Records for unincorporated businesses	Paper or electronic	Five years after 31 January following the year of assessment
Payroll and wage records for companies including PAYE records	Paper or electronic	Six years from the financial year-end in which payments were made
Maternity Records	Paper or electronic	Three years after the end of the tax year in which the maternity pay ends
Current Bank Details	Paper or electronic	No longer than necessary
Any reportable accident, death or injury in connection with work	Paper or electronic	For at least three years from the date the report was made
Records in relation to hours worked and payments made to workers	Paper or electronic	Three years beginning with the day upon which the pay reference period immediately following that to which they relate ends
Disclosure and Barring Service (DBS)	Paper or electronic	Indefinitely if required relevant to ongoing employment. Once the conviction is spent, should be deleted (unless it is an excluded profession)
Immigration Checks	Paper or electronic	Two years after the termination of employment