DATA PROTECTION POLICY

Introduction

Purpose
The Company takes the security and privacy of your data seriously. We need to gather and use information or data about you as part of our business and to manage our relationship with you.

This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

We will be transparent about how we collect and use the personal data of employees, and how we meet our data protection obligations in respect of data privacy and security under the Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR).

This policy applies to the personal data of job applicants, employees, other workers and contractors, and former employees, referred to as HR-related personal data. Note that this policy does not apply to the personal data of clients or other personal data processed for business purposes.

We have appointed Tracy Allen, Group Administration Manager as the person with responsibility for data protection compliance within the Company. She can be contacted at support@monitorservices.co.uk. Questions about this policy, or requests for further information, should be directed to her.

The Company is known as a 'data controller' for the purposes of your personal data, which means that we decide the purpose and manner that personal data is used or will be used.

Definitions
"Personal data" is any information that relates to an individual who can be identified from that information (a 'data subject').
"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical 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.

Data protection principles
The Company processes HR-related personal data in accordance with the following six data protection principles set out in the GDPR:

- To process personal data lawfully, fairly and in a transparent manner.
- To collect personal data only for specified, explicit and legitimate purposes.
- To process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- To keep accurate personal data and take all reasonable steps to update it and to ensure that inaccurate personal data is rectified or deleted without delay.
- To keep personal data only for the period necessary for processing.

- To adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

We are accountable for these principles and must be able to show that we are compliant.

Processing personal data
The Company tells individuals 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 of individuals for other reasons.

Personal data could include recruitment information, such as your application form and CV, your contract of employment, your bank details and information relating to your tax status including national insurance number, identity documents and information relating to your performance and conduct. This is not an exhaustive list.

There are various lawful reasons for processing your personal data set out in the data protection legislation. These may include performance of the contract between us, complying with any legal obligation or if it is in the legitimate interests of the Company. If it is the latter, we can do this if your interests and rights do not override ours and you have the right to challenge our legitimate interests and request that we stop this processing.

Examples of when we might process your personal data can be found in the privacy notice. We will only process special categories of your personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the person for responsible for data protection in the Company.

Under the GDPR, we do not need your consent to process **special categories** of your personal data when we are processing it for the following purposes:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment relationship is held in the individual's personnel file (in hard copy or electronic format, or both) and on HR systems. The periods for which the Company holds HR-related personal data are contained in its privacy notices to individuals.

The Company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the GDPR.

Individual rights
As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests
Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

- whether or not his/her 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 the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the Company has failed to comply with his/her data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, the Company will charge a fee, which will be based on the administrative cost to the Company of providing the additional copies.

To make a subject access request, the individual should send the request to the person with primary responsibility for data protection compliance, Tracy Allen, Group Administration Manager. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify his/her identity and the documents we require. The

Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where large amounts of the individual's data are processed, 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 her if this is the case.

If a subject access request is manifestly unfounded or excessive, we are 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 the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify her that this is the case and whether or not it will respond to it.

Other rights
Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;

- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to Tracy Allen, Group Administration Manager.

Data security
The Company takes the security of HR-related personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

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

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

If you become aware of a data breach you must contact your Manager immediately and retain any evidence in relation to that breach. Under no circumstances should you seek to cover up a breach, or the Company may be unable to act to remedy it promptly and effectively.

International data transfers
We will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities
Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let us know if data provided to us changes, for example if an individual moves house or changes his/her bank details. Individuals may have access to the personal data of other individuals and of our clients in the course of their employment. Where this is the case, we rely on individuals to help us meet our data protection obligations to staff and clients.

Individuals who have access to personal data are required:
- to access only data that they have authority to access and only for authorised purposes;

- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- 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's 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.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.