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 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 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 includes recruitment information, employment records, bank details, tax status, identity documents, performance records, and biometric data collected through the electronic time and attendance system.

The electronic time and attendance system records biometric data (fingerprint, facial recognition) and clocking data (RFID, PIN, mobile app) to monitor attendance, hours worked, and payroll processing. The collection and processing of this data is necessary for employment contract performance, legal compliance, and legitimate business interests.

Employees provide consent to the collection and use of biometric data upon employment. Consent may be withdrawn at any time by notifying your manager or Head Office in writing via email at support@monitorservices.co.uk. Upon withdrawal, alternative clocking methods will be provided.

Retention of Data
Electronic time and attendance records will be retained for 6 years, in line with legal and payroll regulations, after which they will be securely destroyed.
Biometric data (fingerprint and facial recognition) will be deleted immediately upon termination of employment or consent withdrawal.

Data Security & Access
Only authorised personnel (Operations Manager, Area Managers, Contract Managers, Site Supervisors) have access to the electronic time and attendance system reports.

Employees must not share login credentials or allow others to clock in or out on their behalf.

The Company has internal policies and technical controls in place to protect personal data against loss, misuse, or unauthorised access.

Data Breaches
If the Company discovers a data breach that poses a risk to individuals' rights and freedoms, it will report it to the Information Commissioner’s Office (ICO) within 72 hours. If there is a high risk, affected individuals will be informed of the breach and provided with guidance on mitigation.

If you suspect a data breach, notify your Manager immediately and do not attempt to cover it up.

International Data Transfers
We do not transfer HR-related personal data outside the European Economic Area (EEA).

Individual Rights

Employees have the right to:

- Access their personal data (via Subject Access Request to Tracy Allen, Group Administration Manager).
- Request rectification of inaccurate data.
- Request erasure of data no longer needed.
- Restrict processing in certain circumstances.
- Object to processing where legitimate interests do not override individual rights.
- Withdraw consent for biometric data processing under the electronic time and attendance system at any time.

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.