Privacy Policy

DISTRIBUTION

This Privacy Policy is communicated to all employees. A copy is available at the Head Office, held in the sites folder, and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

REVISION HISTORY

Issue Number	Review Date	Changes	Signed
01	22/09/2023	Original version (draft)	
01	22/09/2023	Signed Off	
01	20/09/2024	Review	
01	19/09/2025	Review	
02	20/05/2026	Address Updated	
02	18/09/2026	Review	

INTRODUCTION

ZAM Facilities Management ("the Company") provides security services to its clients. In doing so we collect and use personal data about our employees, job applicants, clients, suppliers, visitors to the sites we protect and members of the public. This Policy explains what personal data we collect, why we collect it, how we look after it and what rights people have over it.

The Policy must be brought to the attention of all Company employees as part of their Induction Training. It is reviewed at least annually, and any amendments must be brought to the attention of all employees.

POLICY STATEMENT

It is the Company's policy to comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations, and to handle personal data fairly, lawfully and with respect. We collect only the information we need, use it only for clear and lawful purposes, keep it secure and delete it when we no longer need it.

WHO WE ARE

The Company is the data controller for the personal data described in this Policy, which means we decide how and why it is used. Where we process data on behalf of a client, for example CCTV or access control at a client's site, the client may be the controller and the Company acts as its processor, under a written agreement. Our address is shown in the footer of this Policy.

SCOPE

This Policy applies to all directors, managers, employees, contractors and agency staff, and to all personal data held by the Company in any form, whether on paper, on a computer or mobile device, on a website, or recorded by CCTV, body-worn cameras or call recording.

PERSONAL DATA WE COLLECT

Depending on the person's relationship with the Company, we may collect:

- **Employees, job applicants and contractors:** name, address, contact details, date of birth, National Insurance number, right to work documents, SIA licence details, CVs, employment history and references, training records, uniform and equipment records, bank details for payroll, emergency contacts, absence and performance records, and photographs for ID badges.
- **Clients and prospective clients:** contact names, job titles, email addresses, phone numbers, site addresses, key-holder details and contract information.
- **Suppliers and subcontractors:** business contact details, bank details and insurance and licence information.
- **Site visitors and members of the public:** names, company names, contact details, vehicle registration numbers, ID checked on entry, and images captured by CCTV or body-worn cameras.
- **Incident and operational records:** names and descriptions of people involved in incidents, daily occurrence logs, patrol and guard-tour records, alarm activation and keyholder call-out records, and statements.
- **Technology and location data:** access control logs, alarm monitoring and control room call recordings, vehicle tracking and lone-worker device location data, and website and email usage data.

Most information comes directly from the person. We also receive some from clients, referees, screening providers, the Security Industry Authority, the Disclosure and Barring Service, government bodies and recruitment agencies.

WHY WE USE PERSONAL DATA

We use personal data only where we have a lawful reason to do so. These reasons are mainly:

- **Contract:** to employ staff, to deliver security services to clients and to deal with suppliers.
- **Legal obligation:** for example right to work checks, tax and payroll, health and safety law, SIA licensing rules and responding to lawful requests from the police.
- **Legitimate interests:** protecting client premises, people and property, preventing and detecting crime, managing incidents, running our business and keeping our staff safe, provided this does not override the person's rights.
- **Consent:** where we have asked for it, for example for certain marketing messages. Consent can be withdrawn at any time.

We do not sell personal data and we do not use it for automated decision-making that has legal or similarly significant effects on people.

SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA

Some information needs extra care. This includes health information, trade union membership, and information about criminal convictions and offences. We collect it only where the law allows

and where it is needed, for example criminal record checks and character vetting for security roles, fitness for work, sickness absence, reasonable adjustments or equal opportunities monitoring. Access is restricted to the few people who need it, and it is kept separately from general personnel records.

SCREENING AND VETTING OF STAFF

Security work requires pre-employment screening, including identity, five-year employment and education history, right to work, SIA licence checks and criminal record checks. People are told what checks will be made before they are carried out. The results are handled in confidence, are seen only by those who need them to make a recruitment decision, and are kept in line with the retention periods below.

CCTV, BODY-WORN CAMERAS AND ACCESS CONTROL

Where CCTV, body-worn cameras or similar equipment are used, clear signs must tell people that recording is taking place, who is responsible and how to contact them. Recording is used only to prevent and detect crime, to protect people and property, to support health and safety and to investigate incidents. Cameras must not be placed where people expect privacy, such as toilets or changing rooms. Staff using body-worn cameras must follow the Company's instructions on when to start and stop recording.

Access to live and recorded images is limited to authorised staff. Footage is only released to the police, the client, insurers or another person where there is a lawful reason, such as a subject access request, a court order or a crime investigation, and every release is logged.

ALARM MONITORING, CALL RECORDING AND TRACKING

Calls to and from our control room may be recorded for training, quality, security and to keep an accurate record of incidents. Vehicles, patrol devices and lone-worker devices may record location data so that we can protect staff, respond to incidents and prove that patrols and visits took place. Staff are told when these systems are in use. Location data is used for these purposes only and is not used to monitor staff outside their working hours.

VISITOR LOGS AND SITE RECORDS

Visitors may be asked to sign in, show identification or give vehicle details. This information is collected to keep the site secure and for fire safety. Visitor books and logs must be kept so that other visitors cannot read previous entries, and must be stored securely.

WEBSITE, EMAIL AND MARKETING

If the Company operates a website, it may use cookies and similar technologies. Non-essential cookies are used only with consent. We send marketing emails or texts only to people who have agreed to receive them or where the law otherwise allows, and everyone can opt out at any time.

SHARING PERSONAL DATA

We only share personal data where necessary and where there is a lawful basis. Recipients may include:

- clients, where information about our staff is needed for site access, vetting or contract compliance;
- regulators and public bodies such as the Security Industry Authority, HMRC, the Home Office and the Disclosure and Barring Service;

- the police and other law enforcement bodies, where there is a lawful request or a legal duty;
- service providers acting on our instructions, such as payroll, IT, training, screening, alarm monitoring and cloud storage providers, who are bound by a written contract; and
- our insurers, auditors and legal advisers.

INTERNATIONAL TRANSFERS

We aim to keep personal data within the United Kingdom. If a provider needs to transfer data outside the UK, we will make sure the transfer is protected by an approved safeguard, such as an adequacy decision or the standard contractual clauses recognised in UK law.

RETENTION

Personal data is kept only for as long as it is needed for the purpose it was collected, or for as long as the law requires. As a general guide:

- unsuccessful job applicant records are kept for one year;
- personnel files are kept for no longer than six years after employment ends;
- payroll and tax records are kept for the period required by law;
- CCTV and body-worn camera footage is overwritten after 31 days unless it is needed for an investigation, a claim or a police request;
- control room call recordings are kept for no longer than 12 months unless needed for an incident;
- visitor logs are kept for 12 months; and
- incident reports and statements are kept for up to six years, or longer where legal action is pending.

Paper records are shredded and electronic records are securely deleted at the end of the retention period.

SECURITY OF PERSONAL DATA

The Company uses appropriate technical and organisational measures to protect personal data. These include locked storage for paper records and removable media, password-protected and encrypted devices, restricted and logged access on a need-to-know basis, secure control rooms and server areas, regular backups and up-to-date security software. Employees must not leave personal data unattended, share passwords, photograph or copy records on personal phones, or send personal data to private email accounts. Personal data must only be sent by secure or encrypted methods.

EMPLOYEES' DUTIES

Security staff often see sensitive information about clients, their staff and members of the public. All employees must:

- keep personal data confidential and only use it for their work;
- only give personal data to the person it relates to, or to someone with proper authority, after checking their identity and the reason for the request, particularly by telephone;
- not access records they have no work reason to see;
- report any lost, stolen or wrongly sent data straight away; and
- pass any request from a person about their data to a Director immediately.

Knowingly or recklessly misusing personal data can be a criminal offence and is a disciplinary matter that may be treated as gross misconduct.

INDIVIDUAL RIGHTS

People whose data we hold have the right to be informed about how we use it, to see a copy of it, to have inaccurate data corrected, to ask for it to be erased, to restrict or object to its use in certain cases, and to receive certain data in a portable format. Requests can be made verbally or in writing to a Director. We will check the identity of the person making the request, will respond within one month and will not normally charge a fee. Where footage shows other people, we may need to hide their images or withhold part of the footage to protect them.

DATA BREACHES

A data breach means any loss, theft, unauthorised access, alteration or disclosure of personal data. Any employee who becomes aware of a breach, or suspects one, must report it to a Director straight away. All breaches are recorded. Where a breach is likely to put people at risk, the Company will report it to the Information Commissioner's Office within 72 hours of becoming aware of it, and will tell the people affected where the risk is high.

RESPONSIBILITIES AND TRAINING

The Directors are responsible for making sure this Policy is followed and that the resources needed to maintain it are available. The Regional Manager is responsible for implementing it at site level. Every employee is responsible for following it. Data protection training is given as part of induction and is repeated regularly.

REVIEW

The Company is committed to progressively improving its data protection practices and will monitor the effectiveness of this Policy with a formal review annually. The Policy will be revised as often as may be appropriate following these reviews.

Managing Director

Name: Danish Iftikhar

Sign: _____

Dated: 22 / 09 / 2023