

**Policy Statement**

Under its obligations to ensure compliance to the general Data Protection Regulations 2018

Taziker is committed to complying with all applicable aspects of Data Protection Legislation. In order to conduct our business activities, we hold personal data about our employees, former employees, job applicants, clients, potential customer prospects, suppliers, and contractors for business purposes. These are not & shall not be shared with any 3<sup>rd</sup> party organisations unless required by law.

**Scope**

This policy applies to the business activities of Taziker, for the processing of personal data in electronic form (including electronic mail and documents created with word processing software); or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

It sets out how we protect personal data and ensures that our employees understand the rules governing their use of personal data to which they have access, in the course of their work (including teleworking) for:

- Compliance with our legal, regulatory, and corporate governance obligations and good practice.
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests.
- Ensuring business policies are adhered to.
- Operational reasons, such as ES related information, recording transactions, operational data such as security CCTV and vehicle tracking in connection with, for example: fatigue management, training and development, quality control, and ensuring the confidentiality of commercially sensitive information, security vetting, and supplier credit reference checking;
- Investigating accidents incidents and complaints.
- Checking references, ensuring safe working practices, monitoring, and managing staff access to systems and facilities, administration, and assessments.
- Marketing our business.
- Improving services.

The Data Protection Policy incorporates several sub policies: -

Data Handling & Security Policy

Personal Data Records Retention Policy

IT Access Controls Policy

IT Data Backup Policy, as well as the company's IMS Procedures, 3.3.1, 3.3.2 & 3.3.3.

**Policy Governance**

The following identifies who within Taziker is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<b>Responsible</b>	Eddie Cairney - Data Privacy Officer
<b>Accountable</b>	James Keenan – Financial Manager
<b>Consulted</b>	Neil Harrison – Managing Director
<b>Informed</b>	All Directors, Managers and Administrative Staff within the business

**Personal Data**

The company may hold information relating to job applicants, current and former employees, agency, contractor and other staff, clients, suppliers, and marketing contacts. Personal data may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV for example.

**Special Category Personal Data**

In our normal course of business, we may also hold personal data about an individual's racial or ethnic origin, trade union membership, health or sexual orientation and biometric data (where used for identification purposes).

**Processing**

Processing refers to the operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Responsibility**

The processing of personal data is ancillary to our core business activities. As such, the business does not undertake the systematic monitoring of data subjects on a large scale, nor does it process large scale special categories of data. However, in-order to promote best practice, Taziker shall ensure compliance through a Data Privacy Officer, who has responsibility for the day-to-day implementation of this policy.

The Data Privacy Officer's responsibilities include:

- Reviewing data protection procedures and policies on a regular basis.
- Advising on data protection training and advice for all employees and those included in this policy.
- Assisting with data protection/handling queries from employees, board members and other stakeholders.
- Receiving and registering a Subject Access Request and directing it to the appropriate divisional head for processing.
- Checking that third parties who handle elements of the company's data, are managing it in accordance with our compliance obligations.

**Data Protection Principles**

Taziker (The Data Controller) is registered with the Information Commissioner's Office, and we process personal data in accordance with the following principles.

Data will be: -

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that personal data that is identified to be inaccurate are either erased or rectified without delay.
- Kept for no longer than is necessary for the purposes for which the personal data are processed.
- Be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures.
- Is not shared with any 3<sup>rd</sup> party organisation unless under an obligation by law.

**Accountability**

Taziker will implement appropriate technical and organisational measures to demonstrate compliance that data is processed in line with principles set out in the GDPR. Internal records of processing activities will typically include the following:

- Name and details of the organisation.

- Purpose(s) of the processing.
- Description of the categories of individuals and personal data.
- Retention schedules.
- Categories of recipients of personal data.
- Description of technical and organisational security measures.
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

The business will implement measures that meet the principles of data protection by design and data protection by default, including data minimisation, and (where possible) pseudonymisation.

### **Lawful Processing**

The legal basis for processing data will be identified prior to data being processed. Data will be lawfully processed under the following conditions, and where applicable, where the consent of the data subject has been obtained for:

- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Where necessary for compliance with a legal obligation.
- Where necessary to protect the vital interests of the data subject or of another natural person.
- Where necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject.

### **Subject Rights**

Individuals (subject to identification verification) whose personal data is held by the business, have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data. Normally, there will be no charge for this, except where a reasonable administration fee may be charged for further copies, or where repetitive, manifestly unfounded, or excessive requests are made by an individual.

Requests should be made to the Data Privacy Officer, and where received, will normally be provided within one month, except where a large number of requests, or especially complex requests are made which may extend the timeframe.

### **Data Handling Requirements**

It is a requirement that all employees and contractors working on behalf of the business, ensure that appropriate security measures are implemented. All electronic documents and records must be stored on the company IT systems, and any hardcopy records must be maintained within the company filing systems. Personal Data or Special Category Data must be kept secure, protected from unauthorised access, and or breach of confidentiality, and must only be made available to authorised persons.

e-mails containing Personal Data or Special Category data files must have the attached file password-protected, and only transmitted to recipients who need such information to carry out their work effectively. A separate email containing the file attachment password details, must be sent. Senders must exercise caution to ensure that when using the carbon copy (cc) function and blind carbon copy (bcc) function, that they are not sending data to an incorrect recipient.

Hard copy paper records of Personal Data or Special Category Data must not be left unattended on work desks or taken off the premises and, must be locked away securely when not being used. Where Personal Data or Special Category Data is being viewed on a computer screen, this must not be left unattended without locking the computer.

The use of removable media (including USB memory sticks, CD's, DVD's) to transfer or temporarily store Personal Data or Special Category Data IS Strictly Forbidden.

**Data Breach Reporting**

A Personal Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. These are categorised as:

**Confidentiality breach**

- where there is an unauthorised or accidental disclosure of, or access to, personal data.

**Availability breach**

- where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

**Integrity breach**

- where there is an unauthorised or accidental alteration of personal data.

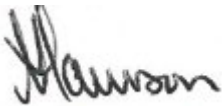
Examples of data breaches include (but are not limited to):

- compromised personal data held by a third-party processor contracted to Taziker.
- unauthorised access to company IT/Filing systems.
- deliberate or accidental action (or inaction) that transfers personal data or special category data by an employee, contractor or third party.
- sending an individuals' personal data to an incorrect recipient.
- loss or theft of computing devices containing personal data.
- loss of availability of personal data due to systems malfunction/deliberate action/extended power outages.

All data breaches are required to be reported to the relevant departmental head, along with a description of the data breach, the numbers of data subjects and categories affected. This includes any loss or theft of any mobile device provided by or authorised for use by the business.

All breaches should be notified to "Responsible" Person, who should maintain a record of such breaches.

This Policy will be reviewed annually to ensure that it reflects current legislation and regulations.

**Neil Harrison**

Managing director

10<sup>th</sup> October 2024