DATA PROTECTION POLICY

Version History

Created By	Philip Johnston
Version	1.2
Last Revision Date	24th January 2022
Last Review Date	24th January 2022
Reviewed By	Philip Johnston

Overview

This policy describes how TOMO Technology will ensure that personal data is collected, handled, stored and disposed of in accordance with applicable data protection laws and regulations. The policy statements apply regardless of whether data is stored electronically, on paper, or on other materials.

The policy is designed to describe the techniques used by TOMO Technology to ensure compliance with relevant data protection laws and regulations. It describes how TOMO Technology maintain compliance to data protection principles as follows:

- **Lawfulness, Fairness and Transparency** - Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose Limitations** - Personal data can only be obtained for 'specified, explicit and legitimate purposes'. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.
- **Data Minimisation** - Data collected on a subject should be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed', i.e. no more than the minimum amount of data should be kept for specific processing.
- **Accuracy** - Data must be 'accurate and where necessary kept up to date'. Data holders should build rectification processes into data management/archiving activities for subject data.
- **Storage Limitations** - Personal data must only be kept in a form which permits identification of data subjects for no longer than necessary.
- **Integrity and Confidentiality** – Controllers and Processors must handle data 'in a manner that ensures appropriate security of the personal data, including protection against unlawful processing or accidental loss, destruction or damage'.

Scope

This policy applies to all personnel employed by, or contracted by, or on behalf of TOMO Technology, and is to be followed during any instance where personal data is being collected, stored or processed.

Definitions

Data Controller - is defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor - is defined as a natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.

Personal Data - is any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Sensitive Personal Data - is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the genetic data, biometric data

for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Identification of Data Processing Operations

As a data controller, TOMO Technology has identified the following data processing activities:

Activity	**Lawful Condition**
Supplier Data - Collection and processing of supplier contact information for the purposes of procuring products and services.	Legitimate Interests
Corporate Customer Data - Collection and processing of personal data related to clients and potential clients for the purposes of providing products and services.	Legitimate Interests
CCTV - Recording of CCTV footage across 16 HD camera's for the purposes of crime prevention and investigation.	Legitimate Interests
HR Data - Collection and processing of general HR data of employees and associates.	Legitimate Interests
HR Data - Collection and retaining of evidence of eligibility to work in the UK	Legal Obligation

It is vital that every employee understands these activities, and understands that any use of personal data which is not covered by this list is flagged to the Managing Director. Failure to do so may well be a breach under GDPR, as the principle of transparency must be applied to all personal data processing activities undertaken, and should we not be declaring a processing activity, we would be in failing to apply that principle.

As a data processor, TOMO Technology has identified the following data processing activities:

Activity	**Lawful Condition**
Customer Data - Collection and processing of personal data related to clients and potential clients for the purposes of providing products and services.	Performance of a contract
Information present on devices – Collection in order to facilitate secure erasure of device data	Performance of a contract

Again, should any other personal data processing activity be undertaken using data provided to us under such agreement, the Managing Director must be informed. We are only allowed to process personal data under the written instructions of the data controller, so any further use of data will need to be discussed and agreed.

Protection of the Rights of Data Subjects

Transparency

When personal data of data subjects is collected, TOMO Technology will provide appropriate information to the data subject.

Where data is collected directly from the data subject, this information will be provided at the time of collection. Where data is not collected from the data subject, this information will be provided to the data subject within one month of the collection taking place.

Privacy Notices covering the data processing activities referred to in the previous section have been covered in the following places:

- Employee privacy notice
- Customer privacy notice – available on the company website.

Security of Personal Data

TOMO Technology will ensure that data privacy is built into business operations, and is considered when personal data processing activities are changed or implemented. Key elements within our Information Security Management System to ensure that this is achieved includes:

- **Appropriate Policies** – All employees need to be aware of their responsibility in order that they handle data carefully to avoid disclosure, loss or unauthorised alteration. TOMO Technology have implemented appropriate policies with regard to information handling and acceptable use of IT assets which must be complied with at all times.
- **Management Commitment, Oversight and Review** – The Senior Management Team is active in communicating the importance of maintaining information security through policies, setting objectives, monitoring non-conformities and reviewing the effectiveness of the ISMS.
- **Information Security Risk Management** – Information Security risks are raised, assessed and treated, according to a formal, documented information security risk assessment methodology.
- **Staff Training and Awareness** – All new staff are provided with training specific to Information Security and Data Protection during induction, while periodic training is provided to all existing staff.
- **Internal Audit** – All applicable controls are subject to periodic review to ensure they are working as intended, are being applied, and are effective.
- **Technical Controls** – A range of technical measures have been implemented, in accordance with ISO 27001:2013 to ensure IT services are secured appropriately.
- **Event, Weakness, Incident and Non-Conformance Reporting** – Staff are made aware of the need to report any actual or potential issues through management channels, and all events and incidents are investigated and remediated according to a formal process.
- **Assessment of Third Parties** – Risk assessments are performed on all third parties in accordance with the Supplier Security Policy. Any acquisition of new technologies, products or services which would involve personal data processing must only be performed in accordance with this policy.

Data Protection Impact Assessments

TOMO Technology will ensure that the impact to data privacy is assessed when personal data processing activities are changed or implemented, and the new or changed activity could pose a high risk to personal data. No such activity is currently performed.

Any impact assessment will include:

- A systematic description of the proposed processing operations.
- The purposes of the processing, including, where applicable, the legitimate interest pursued by the TOMO Technology as the data controller.
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data.

Examples might include:

- Creation of a mobile app that involves systematic profiling of individuals.
- Use of new technologies to host personal data
- A new processing activity that involves large-scale personal data processing

Breach Notifications

TOMO Technology has implemented appropriate Information Security in order that our exposure to any potential incidents is minimized. However, it is recognized that the potential for an incident can never be completely eliminated. TOMO Technology has procedures for this eventuality, as documented in the ***ISMS Manual***.

Should any actual or suspected breach of any personal data be discovered by any TOMO Technology employee, this must be reported in accordance with the documented procedures. Under GDPR, we have a requirement to notify the Information Commissioner's Office of any breach where data subjects are put at risk, so failure to report any such incident could mean we are in breach of this legal requirement.

The Managing Director will ensure that appropriate communication takes place, both to the supervisory authority and to data subjects where necessary. It is also important to note that no other TOMO Technology employee should reveal the extent or nature of any personal data breach to any party outside of TOMO Technology.

Data Protection Officer

The company do not have an appointed Data Protection Officer, as we are not

- a public authority;
- an organisation that carries out large scale systematic monitoring of individuals
- an organisation that carries out large scale processing of special categories of data or data relating to criminal convictions and offences

This is in compliance with GDPR Article 37.1.

Third Parties

Assessment

Any third parties employed by TOMO Technology must be assessed, controlled and monitored to ensure that they are able to assist us in protecting personal data they process on their behalf.

Part of any supplier take-on activity must determine whether the third party will be processing personal data on TOMO Technology's behalf. Where such activities are identified, TOMO Technology will ensure that appropriate contracts, agreements are in place.

All such third parties must be brought on in accordance with the ***Supplier Management Policy*** which forms part of the ***ISMS Manual***.

Where the third party will be processing personal data for which TOMO Technology is not the controller, the results of the assessment will be provided to the data controller.

Data Processing Agreements and Contracts

TOMO Technology must ensure that appropriate Data Processing Agreements and contracts are in place where:

- TOMO Technology is entering into a contract to process personal data on behalf of another data controller (e.g. customers); or
- TOMO Technology is engaging any third party to process personal data on behalf of TOMO Technology.

Data Processing Agreements must reference, as a minimum:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Any contract must reference as a minimum:

- that the processor will only act on the written instructions of the controller;
- that people processing the data are subject to a duty of confidence;
- that the processor will take appropriate measures to ensure the security of processing;
- that the processor will only engage sub-processors with the prior consent of the controller and under a written contract;
- that the processor will assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

- that the processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- that the processor will delete or return all personal data to the controller as requested at the end of the contract;
- that the processor will submit to audits and inspections; and
- that the processor will provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

In order that any third parties employed by TOMO Technology to process personal data do have appropriate coverage in contracts and agreements as detailed above, no employee or business function should sign up to any terms without consulting Managing Director.

Geographical Considerations

TOMO Technology will ensure that, should any personal data be transferred to another country or international organisation, this transfer must be done based on evidential assessment risk-based decision. This will form part of the assessment of any supplier, and a decision as to whether the transfer can be performed be demonstrated though one of the following options:

- **Based on an adequacy decision** – A transfer of personal data to a third country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.
- **Transfer based on appropriate safeguards** – There are multiple options available to allow transfers to be based on 'appropriate safeguards'
    - **Binding corporate rules** – In the case where multi-national suppliers are used, TOMO Technology will assess whether those organisations have BCRs in place and have had those agreements ratified by the relevant supervisory authority.
    - **Model Contract Clauses** – Transfer can be performed should there be a contract in place which ensures that the requirements of data privacy to the levels expected by GDPR have been stipulated.
    - **Evidence of risk assessment and assessment of controls** – Transfers can be conducted as long as evidence is available to show that TOMO Technology has assessed the adequacy of controls and verified that enforceable data subject's rights and effective legal remedies are available.
- **Consent** – Transfers can be made if the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject. TOMO Technology must ensure that there isn't imbalance in the relationship which means consent cannot be freely given.

In order that any geographical issues regarding the geographical third parties employed by TOMO Technology to process personal data do have appropriate coverage in contracts and agreements as detailed above, no employee or business function should sign up to any terms without consulting Managing Director.

Record Retention

In order to comply with the data protection principle that personal data must only be kept for as long as is necessary, TOMO Technology must ensure that clear retention times have been established for each personal data processing purpose identified.

Record retention times to be adhered to are documented in the Records Retention Policy (Appendix A).

Version History

Version Number	Date of change and author	Reason
0.1	9th Oct 2020 – Andy Whillance	Initial draft document created
0.2	3rd Nov 2020 – Philip Johnston	Review and update
0.9	22nd Dec 2020 – Andy Whillance	Final amendments pre approval
1.0	22nd Dec 2020 – Philip Johnston	Approved
1.1	16th Feb 2021 – Andy Whillance	Minor amendment after Stage 1 audit
1.2	24th Jan 2022 – Philip Johnston	Review and update