POLICY OBJECTIVES

- To protect all Personal Information that Tecto is the Controller of or processes on behalf of another Controller.
- To protect the rights and freedoms of the Information
- Subjects whose Personal Information Tecto is the Controller of or processes on behalf of another Controller.
- To ensure appropriate controls are implemented that provide protection for Personal Information, and are proportionate to their value and the threats to which they are exposed.
- To ensure that Tecto complies with and can demonstrate compliance with all relevant legal, customer and other third party requirements relating to the processing of Personal Information in particular the Data Protection Act 1998 and the General Data Protection Regulation (EU 2016/679).

SCOPE

- This policy applies to the processing of Personal Information by any employees or suppliers of Tecto.

RESPONSIBILITIES

- It is the responsibility of the ICT Director to ensure that this policy is implemented and that any resources required are made available.
- It is the responsibility of the QA Co-ordinator to monitor the effectiveness of this policy and report the results at management reviews.
- It is the responsibility of QA Co-ordinator to ensure that a Personal Information Processing Register is maintained.
- It is the responsibility of all employees, to adhere to this policy and report to the ICT Director any issues they may be aware of that breach any of its contents.

DEFINITIONS

Within this policy, the following definitions apply.

- Asset: Any physical entity that can affect the confidentiality, availability and integrity of Personal Information.
- Availability: The accessibility and usability of Personal Information upon demand by an authorised individual.
- Automated decision-making: Processing of information that results in decisions being made about Information Subjects without any review of the information being made by an individual.
- Beyond use: Controls placed on Personal Information that it is no longer necessary for Tecto to keep where it is not reasonably feasible to delete the information. These controls must comply with guidance from the Information Commissioner's Office (see Information Commissioner's Office Guidance on GDPR Compliance).
- Confidentiality: The restrictions placed on the access or disclosure of Personal Information
- Controller: A 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 a set of Personal Information.
- High risk processing: Processing of Personal Information (in particular using new technologies) that is likely to result in a high risk to the rights and freedoms of Information Subjects (see Information Commissioner's Office Guidance on GDPR Compliance).
- Identifiable Natural Person: A natural person who can be identified directly or indirectly, in particular with 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 person.
- Information subject: An Identifiable Natural Person who has Personal Information that Tecto is the Controller of or is a Processor of on behalf of a Controller.
- Integrity: The accuracy and completeness of Personal Information.
- Personal information: Any information relating to an Identifiable Natural Person.
- Personal information protection principles: Principles that shall be applied in relation to all Personal Information as laid down in the Data Protection Act 1998, the General Data Protection Regulation (EU 2016/679) and any subsequent amendments.

TectoGroup®
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF

T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk

Registered in England & Wales No: 07923637

- Processor: A natural or legal person, public authority, agency or other body which processes Personal information on behalf of a Controller.
- Security incident: Any event that has a potentially negative impact on the confidentiality and/or integrity and/or availability of Personal Information or restrict the rights and freedoms of Information Subjects.

ACCOSIATED DOCUMENTS

- All associated documents referred to in this policy are highlighted in bold and underlined.

POLICY

Application of the Personal Information protection principles

- The following principles must be applied and compliance with them demonstrated in relation to all Personal Information that is accessed, stored or processed by employees, and employees or suppliers, while they are accessing or processing the Tecto's information assets and any Personal Information that Tecto is the Controller of or processing on behalf of another Controller:
- Personal information shall be processed lawfully, fairly and in a transparent manner;
- Personal information shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- Any Personal Information collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Any Personal information processed shall be accurate, kept up-to-date (where necessary) and every reasonable step is taken to ensure that Personal Information that is inaccurate with regards to the purposes for which it is processed is erased or rectified without delay;
- Personal information shall not be kept in form that permits identification of Information Subjects for longer than is necessary for purposes for the which the personal information is processed (Personal Information may be put Beyond Use where deletion is not reasonably feasible);
- Appropriate technical and organisational measures shall be taken to ensure appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage;
- All processes and operations that involve the processing of Personal Information must be designed to ensure that these principles can be achieved and are applied. Where any changes are required to Tecto's Assets that impact on the processing of Personal Information, a review of the Control Measures applied must be complete.

Registration with the Information Commissioner

- It is the responsibility of the QA Co-ordinator to ensure that the appropriate registration is maintained with the Information Commissioner.

Personal Information Processing Register

- A Personal Information Processing Register must be maintained that contains information on
- All Personal Information that Tecto is the Controller of regardless of whether it is processed by Tecto or by a Processor engaged by Tecto;
- All Personal Information that Tecto is a Processor of on behalf a Controller or other Processor;
- The types of Information Subjects that the Personal Information relates to, the limit of the information collected and the source that it is obtained from;
- The reason the processing is undertaken and the legal grounds for doing so;
- The types of processing employed and the methods and technologies used;
- The details of any Processers used (where Tecto is the Controller) or direct Sub-Processors used (where Tecto is the Processor);
- The country or region where the Personal Information is processed and stored;
- All recipients of the Personal Information;
- The period for which the Personal Information is retained and the justification for doing so;

TectoGroup®
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF
T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk
Registered in England & Wales No: 07923637

- Whether any Automated Processing is undertaken;
- Whether the Personal Information falls into a Special Category and if so the processing justification offered by Article 9 of the General Data Protection Regulation (EU 2016/679) that applies.
- Whether the Personal Information is transferred in any way outside of the EU and if so the countries/ territories/organisations it is transferred to.

Consent to process Personal Information

- Where Tecto is a Controller of Personal Information and it undertakes processing of Personal Information requiring the consent of the Information Subject, a record of the consent must be obtained from the Information Subjects using a Privacy Notice + Consent Opt-in Form.

Processing of Personal Information Obtained from an Information Subject

Where Tecto has collected personal data directly from an Information Subject, they must be provided with a Privacy Notice that contains at least the following information:

- The name and contact details of ICT Director
- The scope and legal justification of processing that will be undertaken with the information they provide;
- Where the legal justification for processing the Personal Information is the Controller's legitimate interest, details of the legitimate interest;
- Where the legal justification for Processing the Personal Information is that the Information Subject has consented to the processing, the existence of a right to withdraw consent at any time, without affecting the lawfulness of the processing carried out prior to the withdrawal;
- The categories of recipients who will have access to their Personal Information;
- The time period for which their information will be stored or the criteria that will be applied to determine the time period;
- Any planned transfers of their information to a third country or international organisation and information on the safeguards being applied and the means by which the Information Subject can obtain a copy of them or where they are available;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- Whether any automated decision-making will be applied to their information and if so the logic that will be applied and the envisaged consequences for them;
- Whether Tecto is a joint Controller of the information and if so and overview of the agreement in place with other joint Controllers;
- Their rights to:
    - request access to their information
    - request corrections be made to their information
    - request their information be deleted
    - request that processing of their information is restricted
    - request their information be transferred to another Controller
    - lodge a complaint with the Information Commissioner and the means by which they can notify Tecto to exercise one or more of these rights;

Processing of Personal Information obtained from third parties;

- Where Tecto is a Controller of Personal Information and it undertakes processing of Personal Information obtained from a third party (i.e. not directly from the Information Subjects it relates to) then unless:
- The Information Subject already has the information that Tecto has obtained; or
- The collection or disclosure of the information is authorised or required by EU or UK law; or
- The disclosure of the information is restricted by due to the obligation of a professional body that has provided it or a requirement of EU or UK law;

TectoGroup®
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF
T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk
Registered in England & Wales No: 07923637

- It would require a disproportionate effort to provide the information.
- This information will be provided to Information Subjects either within one month of Tecto obtaining the information or at the time of first communicating with the Information Subject (whichever is the soonest).

Accessing, processing and storage of Personal Information

- ICT Director must ensure that appropriate physical and technical controls are in place to:
- Protect to confidentiality, integrity and availability of all Personal Information;
- Prevent unlawful processing of Personal Information.

Personal information should be accessed, processed and stored only to:

- Fulfil the needs of customers;
- Comply with legal requirements;
- Enable the effective implementation of the organisation's ISMS.
- Access to Personal Information must be provided in only where is necessary for individuals to undertake tasks assigned to them that require access.

Requests by Information Subjects to exercise their rights and freedoms for all Personal Information that Tecto is the Controller of:

- All requests by Information Subjects whose Personal Information is processed by Tecto, to exercise their rights and freedoms under the Data Protection Act 1998 and the General Data Protection Regulation (EU 2016/679) will be managed in accordance with the Handling of Personal Information Requests Procedure.
- Any information that needs to be provided to Information Subjects who submit requests will be provided in a concise, transparent, intelligent and easily accessible form, using clear and plain language.
- Any information requested by Information Subjects in the relation to any of their Personal Information processed by Tecto that Tecto is legally obliged to provide, will be provided free of charge unless the request if manifestly unfounded or excessive, in which case Tecto may change a reasonable fee for providing the information of refuse to act on the request.
- Where the request covers the deletion of information that has been made public then Tecto will take all reasonable steps possible to inform other Controllers who are processing the information to delete any copy of the information that they hold or any links they have to the information.

Transferring Personal Information

- Any transfer of personal information to a third party must be carried out under a written agreement, setting out the scope and limits of the sharing.
- In the event that Tecto needs to transfer Personal Information to a non-EU country or an international organisation then:
  - The relevant Privacy Notices need to identify this;
  - The Information Subjects affected must be informed before the transfer takes place and provided with information regarding the safeguards that Tecto will ensure are in place.

Compliance and Controls Assessments

- To ensure that:
  - All controls employed to protect Personal Information is controlled or processed by Tecto are maintained and effective;
  - Tecto complies with the Data Protection Act 1998 and the General Data Protection Regulation (EU 2016/679);
  - Audits will be completed annually and the results recorded using the Active Legal Compliance Manager.

Arrangements with Joint Controllers

- Where Tecto is a joint Controller of any Personal Information then a Joint Controller Agreement (or an equivalent agreement) will be implemented with any joint Controllers;

TectoGroup®
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF
T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk
Registered in England & Wales No: 07923637

Arrangements with Controllers

Where Tecto undertakes processing on behalf of a Controller

- A Personal Information Processing Agreement (or an equivalent agreement) will be implemented with any Processors.
- No processing of information provided by the Controller will be undertaken without an explicit instruction from them.

Arrangements with Processors

Where Tecto uses a supplier to undertake processing on its behalf:

- A Personal Information Processing Agreement will be (or an equivalent agreement) will be implemented with any Processors;
- A Personal Information Processor Assessment will be completed to assess whether they can provide sufficient guarantees to implement appropriate control measures that will ensure the processing they undertake complies with the Data Protection Act 1998 and the General Data Protection Regulation (EU 2016/679) and protects the rights and freedoms on the Information Subjects whose information they process on behalf of Tecto.

An audit of a supplier's compliance with the Data Protection Act 1998 and the General Data Protection Regulation (EU 2016/679 will be undertaken where:

- The information obtained from a Personal Information Processor Assessment raises doubts as to the adequacy of the guarantees provided by a Processor; or
- The supplier is undertaking High Risk Processing; or
- A Personal Information Breach occurs that has a significant impact on the confidentiality or integrity or availability of any Personal Information and following an investigation of the root cause of the incident, the controls and processes employed by the supplier are identified as having been a contributing factor.
  The audit will be completed using the Activ Legal Compliance Manager.

High Risk Processing

- A data impact assessment must be completed for any High Risk
- Processing of Personal Information that Tecto is a Controller of before any such processing is started.
- The results of the data impact assessment must be recorded in the
- Personal Information Processing Register.
- If a data impact assessment indicates that the processing would result in a high risk to the rights and freedoms of the Information Subjects whose Personal Information is being processed, then QA Co-ordinator must consult with the Information Commissioner's office before any processing is started

Personal Information Breaches

- In the event of a Security Incident that compromises the confidentiality, integrity of availability of any Personal Information actions shall be taken and records maintained in accordance with the Security Incident Management Procedure.

Joint Review

- This policy shall be reviewed at least annually or if significant changes occur that might affect its continuing suitability, adequacy and effectiveness.

Signed on behalf of Tecto Ltd: Ben Calder

Position: Director

Date: December 2024

TectoGroup®
Unit 2 Spinney View,
Round Spinney Ind Est
Northampton NN3 8RF

T 01604 961 961
E info@tecto.co.uk
W www.tecto.co.uk

Registered in England & Wales No: 07923637