**Company Data Protection Policy**

*IMPORTANT NOTICE*

*This document does not constitute legal advice. It should be tailored to reflect your specific requirements and usage of data following a data audit in accordance with the legislation, guidance and Codes of Practice issued by the Information Commissioner. This policy is designed to be used in conjunction with an appropriate Privacy Policy, Data Retention Policy and a Data Security Policy.*

# Purpose, Scope and Users

[*insert name of data controller*] ('we' or 'us') are a 'data controller' for the purposes of the relevant data protection legislation including the Data Protection Act 1998, the General Data Protection Regulations and any subsequent legislation as appropriate.(i.e. we are responsible for, and control the processing of, your personal information).

This Policy sets forth the basic principles by which we processes the personal data of customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of our business departments and employees while processing personal data.

This Policy applies to the Company and its directly or indirectly controlled wholly-owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

This policy is designed for use by all officers, employees, servants or agents whether permanent or temporary, as well as all independent contractors working on our behalf.

#

# Reference Documents

* Relevant data protection legislation including the Data Protection Act 1998, the General Data Protection Regulations and any subsequent legislation as
* [INSERT COMPANY POLICIES HERE. these can include,
* *Privacy Policy*
* *Employee Personal Data Protection Policy,*
* *Data Retention Policy,*
* *Data Subject Access Request Procedure]*

# Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union’s General Data Protection Regulation:

**Personal Data**: Any information relating to an identified or identifiable natural person ("Data Subject") 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**: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.

**Data Controller**: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

**Data Processor**: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

**Processing**: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

**Anonymization**: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

**Pseudonymization**: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymization reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

**Cross-border processing of personal data**: Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

**Supervisory Authority**: An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR;

# Basic Principles Regarding Personal Data Processing

These data protection principles outline the basic responsibilities for The Company and how we handle personal data. All personal data will be processed in line with the nation data protection laws in place at the time of the processing. Including, but not limited to the GDPR. The Company will process any personal data in line with these principles, including.

* Lawfulness, Fairness and Transparency- Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
* Purpose Limitation- Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
* Data Minimization - Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The Company must apply anonymization or pseudonymization to personal data if possible to reduce the risks to the data subjects concerned.
* Accuracy- Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.
* Storage Period Limitation - Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.
* Integrity and confidentiality- Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, the Company must use appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.
* Accountability - Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

# Data Protection and Security

Our policies, guides and processes are designed to ensure that the principles of data protection are built in by design. These principles include:

* 1. **Data subjects choice and consent**

That data subjects are informed of the nature of any data processing and that where appropriate any consents are informed (See the Fair Processing section.)

* 1. **Collection**

That only the least amount of personal data reasonably required is collected. If personal data is collected from a third party, the Company must ensure that the personal data is collected lawfully.

* 1. **Use, Retention, and Disposal**

The purposes, methods and retention period of personal data must be consistent with the information provided to the data subject. We must maintain the accuracy, integrity, confidentiality and relevance of personal data based on purpose for which the data was obtained. Adequate security processes must be followed to protect personal data and prevent personal data from being stolen, misused, or abused, and prevent personal data breaches.

* 1. **Disclosure to Third Parties**

Where the Company uses a third-party to process personal data on its behalf, the Company must ensure that this processor will comply with the requirements of the GDPR and provide sufficient security measures to safeguard personal data as appropriate.

The third-party partner must only process personal data to carry out its contractual obligations towards the Company or upon the instructions of the Company and not for any other purposes.

When the Company processes personal data jointly with an independent third party, the Company must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document.

* 1. **International Transfer of Personal Data**

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards must be used, including the signing of a Data Transfer Agreement, as required by the European Union and, if required, authorization from the relevant Data Protection Authority must be obtained.

* 1. **Rights of Access by Data Subjects**

When acting as a data controller, the Compliance Manager is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure.

* 1. **Data Portability**

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free. The Compliance Manager is responsible to ensure that such requests are processed within one month, are not excessive and do not affect the rights to personal data of other individuals.

* 1. **Right to be Forgotten**

Upon request, Data Subjects have the right to obtain from the Company the erasure of its personal data. When the Company is acting as a Controller, the Compliance Manager must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

# Fair Processing

The Company must decide whether to perform a Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines. Personal data must only be processed when authorised and in line with this policy.

* 1. **Notices to Data Subjects**

 When collecting personal data for any kind of processing activities, including but not limited to selling products, services, or marketing activities, the Company will properly inform data subjects of : the types of personal data collected, the purposes of the processing, processing methods, the data subjects’ rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the security measures taken to protect personal data. This information is provided through our Privacy Notice.

 Where personal data is being shared with a third party, the Company must ensure that data subjects have been notified of this through a Privacy Notice.

 Where sensitive personal data is being collected, the Compliance Manager must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected.

* 1. **Obtaining Consents**

 Whenever personal data processing is based on the data subject's consent, or other lawful grounds, The Company is responsible for retaining a record of such consent. You must ensure that data subjects are sufficiently informed and ensure that they are aware that their consent can be withdrawn at any time.

 Where the Company collects the personal data of a child under the age of 16, you must ensure that parental consent is obtained and recorded.

 Personal data must only be processed for the purpose for which they were originally collected. In the event that the Company wants to process collected personal data for another purpose, the Company must update any consents and inform the data subject. Any such communication should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s).

# Organization and Responsibilities

Everyone who works for or with the Company and has access to personal data processed by the Company has the responsibility for ensuring appropriate personal data processing.

The key areas of responsibilities for processing personal data lie with the following organisational roles:

**The Board of Directors** makes decisions about, and approves the Company’s general strategies on personal data protection.

**The Data Protection Officer (DPO)**, is responsible for managing the personal data protection program and is responsible for the development and promotion of end-to-end personal data protection policies.

**The IT Manager,** is responsible for ensuring all systems, services and equipment used for storing data meet acceptable security standards and performing regular checks to ensure the continued integrity and functionality of all hardware and software

# Subject Access, Correction or Requests To Delete Data

When requests to access, correct, amend or destroy personal data records, You must ensure that these requests are handled within a reasonable time frame and in any event no longer than 40 days. The Company must also record the requests and keep a log of these.

# Response to Personal Data Breach Incidents

When the Company learns of a suspected or actual personal data breach, the matter must be reported to the Data Protection Officer at the earliest opportunity. The Data Protection Officer must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the Data Breach Policy. Where there is any risk to the rights and freedoms of data subjects, the Company must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

# Audit and Accountability

The company will auditing how well business departments implement this Policy. Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

#  Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which the Company operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.