Data protection policy

This policy sets out how [COMPANY NAME] handles the personal data of its employees, customers, suppliers and other third parties.

This policy is intended to ensure that we:

- Comply with data protection law and follow good practice;
- Protect the rights of team members, customers and partners;
- Are transparent about how we store and process individuals' data;
- Are protected from the risks of a data breach.

Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. This policy is therefore intended to apply to the personal data that we process about you. It also applies to you in situations where your role involves you processing data on our behalf.

This policy does not form part of any employee's contract of employment, and we may amend it at any time. It does not override any applicable national data privacy laws and regulations in countries where we operate.

Scope

This policy applies to all personal data that we process regardless of the media on which that data is stored, or whether it relates to past or present employees, workers, customers, suppliers, or any other data subject.

Anyone who works for the Company, whether or not they are employees, must read, understand and comply with this document when processing personal data. Any breach of the rules contained within this policy may result in disciplinary action.

Data protection principles

We adhere to the principles relating to the processing of personal data, as set out in the GDPR. These require personal data to be:

- Processed lawfully, fairly and in a transparent manner;
- Collected only for specified, explicit and legitimate purposes ("purpose limitation");
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ("data minimisation");
- Accurate, and where necessary, kept up to date ("accuracy");
- Not kept in a form which permits identification of data subjects for longer than is necessary ("storage limitation");
- Processed in a way which ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing, and against accidental loss, destruction or damage ("integrity and confidentiality");

In addition to these 6 core principles there are a number of other obligations on us (as the controller of your data) and rights that you have in relation to your data (as data subject). These include requirements that your personal data is:

- Not transferred to another country without appropriate safeguards in place;
- Made available to data subjects, who must be allowed to exercise certain rights in relation to their personal data.;

Fair, lawful and transparent processing

We must process your personal data lawfully, fairly and in a transparent manner.

What this means is that we can only process your data fairly and lawfully and for one of the specified purposes (or legal bases) set out in the GDPR. These include the following:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

When we collect personal data about you, whether directly from you or from a third party, then we are obliged to provide you with certain information about that personal data including what we will do with it, who we will share it with and what our legal basis for processing is. That information will be set out in a Privacy Notice (or similar).

Consent

We can only process personal data on the basis of one or more of the lawful bases set out in the GDPR, and listed above - these include with the consent of the data subject.

Consent can be difficult to obtain under the GDPR. It must freely given, specific, informed and unambiguous.

In order to consent to the processing of their personal data, a data subject should indicate their agreement either by a statement or by positive action. You cannot assume that consent has been given in the absence of any express agreement.

Data subjects must be easily able to withdraw their consent at any time. We will keep records of all consents, so that we can demonstrate our compliance with this data protection requirement.

Accountability

We are the Data Controller (or simply Controller) for your data. As the Controller we are responsible for implementing appropriate technical and organisational measures to ensure compliance with the data protection principles detailed above.

As part of that responsibility we will appoint a person(s) to be responsible for data protection and we may appoint a suitably qualified Data Protection Officer. We will also take a number of other steps, including to:

- Ensure and document GDPR compliance;
- Train Company personnel on the GDPR and on our associated policies and procedures.

Purpose Limitation

When we collect personal data it must be only for explicit and legitimate purposes that are clear up front. We may not process the data in any manner that is incompatible with these purposes.

If the purposes for data collection and processing change, then we must inform the data subject of these new purposes, and if necessary, we must gain their renewed consent.

Data Minimisation

The data that we collect and process must be limited to what is strictly necessary and relevant for the intended purposes. When any data is no longer needed for these purposes, we must then either delete or anonymise it.

Accuracy

We must check the accuracy of any personal data at the point of collection, and at regular intervals afterwards, and either delete or correct inaccurate or out-of-date personal data.

Storage Limitation

Personal data must not be kept in an identifiable form for any longer than is necessary for the stated purposes for which the data is processed. Therefore, we must ensure that when personal data is no longer needed, it is deleted or anonymised. We will require third parties to also delete or anonymise data where and when applicable.

Integrity and Confidentiality

We must secure personal data by taking technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Such safeguards may include the use of encryption and pseudonymisation. We will exercise particular care in protecting special categories of personal data and criminal convictions data.

Personal Data Breaches

Should a breach of personal data occur, we will usually notify the appropriate regulator (unless it is assessed that the breach is unlikely to result in a risk to the rights and freedoms of individuals) and, in certain instances, the data subject. We are also obliged to keep a record of all personal data breaches.

Data subjects' rights

The people whose data we hold (data subjects) have many rights regarding the processing of their personal data. These include, but are not limited to, the following rights to:

- Withdraw consent to the processing of their personal data;
- Request access to their personal data that the company holds;
- Prevent our use of their personal data for direct marketing purposes;
- Ask us to erase any personal data that is no longer necessary for us to hold;
- Ask us to correct any inaccurate or out-of-date data;
- Prevent processing of data that is likely to cause damage or distress to the data subject or to anyone else;
- Be notified of a data breach which is likely to result in high risk to their rights and freedoms.

Record keeping

We are required by law to keep full and accurate records of all our data processing activities. These records include:

- Data subjects' consents to the processing of their personal data;
- The name and contact details of our Data Protection Officer, if applicable;
- Clear descriptions of the types of data that we hold, and of the types of data subjects whose data we hold;
- The purposes of our data processing;
- The categories of recipients to whom the personal data has or will be disclosed;
- Details of any third-party recipients of personal data;
- Where possible the envisaged time limits for erasure of the different categories of data;
- Where possible, a description of the security measures in place.

Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers. Customers generally need to give us their consent for us to send them electronic direct marketing communications, for example via emails, texts or automated calls. If a customer opts out of receiving direct marketing communications, we must honour their request promptly.

Sharing personal data

You should generally only share personal data with third parties, such as service providers, under the following circumstances:

- The third party needs to hold the data in order to provide the contracted services;
- The privacy notice given to the data subject has made it clear that their data will be given to third parties for express purposes;

- The third party has agreed to comply with the necessary data security standards and procedures;
- There exists a GDPR compliant contract between both parties.
- The transfer of data complies with cross-border transfer restrictions.

You may only share personal data with other employees or agents of the Company if the recipient needs to have the data in order to fulfil their role.