Data Protection Policy

Contents

1. **Policy Statement**
    a. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our clients, employees and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.
    b. Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. **About This Policy**
    a. The types of personal data that All Mastic Limited (referred to as "we", "our" or "us" in this policy) may be required to handle include information about current, past and prospective clients, employees and other third parties that we communicate with. The personal data, which may be held on paper or on a computer or other media, is currently subject to certain legal safeguards specified in the General Data Protection Regulations (the "Regulations").
    b. This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.
    c. This policy replaces any previous data handling policies in force at All Mastic Limited.

d. This policy does not form part of any employee's contract of employment and may be amended at any time. We will usually give you notice of amendments to this policy.
e. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.
f. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to John O'Connor, Data Protection Compliance Manager, All Mastic Ltd, Harbour Road, Portishead, Bristol, BS20 7BL.

3. Definition Of Data Protection Terms

a. "Data" is information which is stored, for example, electronically, on a computer, or in paper-based filing
b. "Data subjects" for the purpose of this policy includes an identified or identifiable natural person
c. "Personal data" means any information relating to a data subject or from which a data subject can be identified by. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about the data subject, their actions or behaviour.
d. "Data controllers" are the people / organisations which determine the purposes for which, and the manner in which, personal data is processed. We are the data controller of all personal data used in our business for our own commercial purposes.
e. "Data users" are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this policy at all times.
f. "Data processors" include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. We will in some circumstances be a data processor in relation to personal data provided to us by third parties if we are processing the data on their behalf.
g. "Processing" is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
h. "Special categories of personal data" are categories of personal data which additional regulations apply to and include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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.

4. Data Protection Principles

a. Anyone processing personal data must comply with the following principles. Personal data must be:
    i. Processed lawfully, fairly and in a transparent manner.

ii. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
iii. Adequate, relevant and limited to what is necessary in relation to those purposes.
iv. Accurate and where necessary, kept up to date.
v. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
vi. Processed in a manner that ensures appropriate security of the personal data.

b. As a data controller, it is our responsibility to demonstrate compliance with those principles.
c. Under no circumstances should personal data be processed in breach of the above principles. Please contact the Data Protection Compliance Manager, if you think there may have been a breach of the above principles.
d. In addition to the above principles, personal data must not be transferred outside of the European Economic Area ("EEA") without satisfying certain criteria. It is our policy that no-one processing personal data within our organisation should transfer data outside of the EEA without the data subjects' explicit consent. In order to be able to transfer personal data outside of the EEA, you must ensure:
    i. You have explained to the data subject why we wish to transfer their data outside of the EEA;
    ii. You have explained to the data subject the ramifications of sending the personal data outside of the EEA, for example, that the third party country may not have as protective data protection legislation which could result in personal data being used for purposes for which it was not provided;
    iii. The data subject has given consent to the specific transfer and the specific purposes for which the data will be used;
    iv. The data subject has given a clear and unambiguous indication of their consent.
e. We must be able to demonstrate that the data subject provided their compliant explicit consent to transfer their personal data outside of the EEA and so telephone notes or emails demonstrating the data subject's explicit consent must be made or retained.
f. Under no circumstances is personal data to be transferred outside of the EEA without compliant consent of the data subject or authority of the Data Protection Compliance Manager.

5. Processed Lawfully, Fairly And In A Transparent Mananer

a. This principle is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.
b. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data

controller or the party to whom the data is disclosed. When any special categories of personal data are being processed, additional conditions must be met.

c. When processing personal data in the course of our business, we will ensure that those requirements are met.

6. Collected For Specified, Explicit and Legitimate Purposes

a. In the course of our business, we may collect and process a variety of personal data including, for example, candidates' CVs, addresses, qualification details and contact details.

b. We may receive personal data directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, clients, business partners, contractors, sub-contractors in technical, payment and delivery services, credit and criminal reference agencies and others).

c. We will only process personal data for the specific purposes for which it was collected or for any other purposes specifically permitted by the Regulations.

d. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. Adequate, Relevant and Limited To What Is Necessary

a. We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject and will not collect more personal data than we need in relation to that specific purpose.

8. Accurate and Up to Date Data

a. We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9. Timely Processing

a. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10. Data Security

a. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

b. We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

c. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

i. Confidentiality means that only people who are authorised to use the data can access it.
ii. Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
iii. Availability means that authorised users should be able to access the data if they need it for authorised purposes.

d. Security procedures include:
    i. Entry controls: Our offices are not entry controlled, but we do not however share the building with any other business. Any stranger seen in our offices should be reported.
    ii. Secure lockable desks, cupboards and filing cabinets: Desks, cupboards and filing cabinets should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
    iii. Methods of disposal: Paper documents contained personal data should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
    iv. Equipment: Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
    v. Digital devices:
        1. Your personal digital devices:
            a. All Mastic's computer system must only be accessed using your secure login in details; and
            b. You may access the secure login in portal from your own personal devices, but you are not permitted to download anything from the portal to your desktop (or equivalent) or send work emails from your personal accounts.
        2. All Mastic's digital devices:
            a. All Fastglobe mobiles and laptops must be encrypted and password protected and the passwords must be changed every 6 months; and
            b. You must ensure that your All Mastic mobile devices have the "Find My iPhone" app or equivalent installed to assist in locating lost devices or to allow the content to be erased if the device cannot be found.

11. Notifying Data Subjects

a. If we collect personal data directly from data subjects, we will inform them about:
    i. The purpose or purposes for which we intend to process that personal data.
    ii. The types of third parties (e.g. clients), if any, with which we will share or to which we will disclose that personal data.
    iii. The means, if any, with which data subjects can limit our use and disclosure of their personal data.
b. If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

c. Where relevant, we will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

12. Data Subjects Rights

a. We will process all personal data in line with data subjects' rights, in particular their right to:
    i. Request information on what personal data we hold about them and provide access to it.
    ii. Prevent the processing of their data for direct-marketing purposes.
    iii. Ask to have inaccurate data amended, erase data we hold about them or restrict the types of process we carry out in respect of that data.
    iv. Request we provide the personal data we hold about them in order they can use it for their own purposes across other services.
b. If the data subjects exercise any of their above rights, before doing anything, please contact the Data Protection Compliance Manager whose details are set out in clause 2.f. immediately in order they can assist you with how to proceed.
c. When receiving enquiries, we must not disclose personal data we hold on our systems unless we have checked the enquirer's identity to make sure that information is only given to a person who is entitled to it.
d. Employees should not be coerced into taking action in relation to a data subjects' personal information under any circumstances without being sure it is appropriate to do so as this in itself could result in a breach of the applicable legislation.

13. Changes To This Policy

a. We reserve the right to change this policy at any time.

Directors Signature:  **Date: 8 August 2023**