DATA PRIVACY POLICY

February 2021

Contents

1 PURPOSE

The purpose of this policy is to set out our responsibilities and methodologies for processing all types of personal and sensitive data throughout the organisation. It outlines our compliance to the Data Protection Act 2018 incorporating the General Data Protection Regulation (GDPR) and our data protection responsibility to any third parties we are in contact with. H. A. Marks Limited and other companies within the Group are referred to hereinafter as 'the Company'.

Data protection legislation prescribes the way in which the Company may collect, retain and handle personal data. The Company complies with the requirements of data protection legislation and all employees who handle personal data in the course of their work must also comply with it.

The Company processes personal data for individuals that work for and on behalf of the company, including those that have left. The Company also may process personal data and sensitive data that refers to third parties involved in our work.

As this policy defines the Company's overall data protection and privacy policy, it also encompasses the sensitive information associated with our projects, including but not limited to site access and site plans. Sensitive data relating to projects is hereinafter referred to as 'sensitive project data' and is distinct from 'sensitive personal data'. The Data Protection Act (2018) refers to special categories of personal data as 'sensitive data' and is covered in more detail under 3.2. This policy also covers areas of IT within the company.

2 RELATED DOCUMENTS

This policy is a part of a set of policies that cover all aspects of privacy including access to and authentication with our computer systems. All staff should make themselves aware of all privacy and security polices relevant to their job outlined in the H.A. Marks Ltd Employee Handbook.

Other related documents include the Data Privacy Policy (available publicly on our website), Subject Access Requests procedure and the Data Breach procedure. Other procedures referred to include the Company's disciplinary procedure.

3 RESPONSIBILITY & SCOPE

3.1 Responsibility

Company policy dictates that under no circumstances should any personal data of any category be shared with any other party unless it is an essential requirement of the Business, the Employee or Contractor. This policy also dictates that sensitive project data should only be shared with those authorised to receive it. Such authorisation to be given by those leading the project.

As an external receiver of personal data held by us must also be compliant with Data Protection Act 2018 incorporating GDPR (apart from an individual making a request on their own data), then we require assurance on how they intend to process the data. If in any doubt,

discuss the issue with the company's Data Controller before releasing the personal data requested. All personal data must be treated as highly confidential.

The Company do not subject personal data to automatic processing or profiling other than for the purposes of allocating expertise to specific jobs.

It is the responsibility of the Director to ensure that this Policy is updated to reflect identified changes resulting from the Company's review process.

- The Director in accordance with this Policy will make any changes to this Policy, or issue of authorised changes.
- It is the responsibility of all staff to ensure that they are both familiar with this Policy/Procedure and that they are working to the current issue of documentation.
- It is the responsibility of all staff to keep their personal data accurate and up to date.

3.2 Scope

- "Personal data" is any information that relates to a living individual who can be identified from that information.
- "Processing" is any use that is made of personal data, including collecting, storing, amending,
- "Special categories of personal data" or "Sensitive personal data" means information about an individual's racial or ethnic origin, political opinions, religious or political beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
- "Sensitive project data" is any information that relates to access details or site plans for projects both past and current.
- "Criminal records data" means information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.
- "Employee" includes employees, direct contractors, volunteers, interns and / or apprentices.

4 METHOD

4.1 Data Protection Team

The Data Protection Team (consisting of the Data Controller, Directors, Payroll Manager, Office Manager and Senior Contracts Managers) are responsible for providing overall direction. It ensures the company keeps a record of its processing activities in respect of all personal and sensitive data.

4.2 Security of Data

The Company will ensure that personal data is not processed unlawfully, lost or damaged. If any employee has access to personal data during the course of their employment or contractual engagement, they must also comply with this obligation. If an employee believes they have lost any personal data in the course of their work, it must be reported to their manager immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

4.2.1 Digital records

Data is mainly stored on the Company's IT systems and is therefore an intrinsic component of Data Protection and Privacy. Employees are advised to read and strictly adhere to the Company's IT Policy. All Personal Data and sensitive project data must reside on the Company's servers and only access by authenticated users. No personal data or sensitive project data should be stored on individual PCs, Laptops, Tablets or PDAs. Site access information can be copied and held on a personal device whenever employees require access to that site, but the data held should not state the actual site address and the Laptop, Tablet or PDA must be password or passcode protected with a locking time of less than 121 seconds. For the purposes of this policy document, a synopsis of the relevant sections of the Company's IT policy:

- access to PC's and Laptops is protected by strong passwords that are changed frequently;
- all devices connected to the internal network must have an automatic time of inactivity lock with a password required to restart activity;
- all personally carried data devices must, when outside the Company's premises, have an automatic locking system that stops access and requires a security code to regain access. Where the system contains sensitive project information that time of inactivity before locking should be no longer than 121 seconds;
- wherever possible and always on systems taken out of the Company's premises, data is encrypted;
- access to servers is only permitted to IT personnel.

For information purposes:

- access to all infrastructure devices is protected by strong passwords (not the supplier's default) and employees other than IT personnel are not permitted to access;
- penetration testing for external facing infrastructure equipment is carried out at least once per year;
- penetration testing for wireless access points is carried out at least once per year;
- remote access is via a minimum of 2-tier authentication.

4.2.2 Hard Copy Records

Some personal data will be provided and hard-copy and where necessary will be scanned and stored as a digital record. Hard-copy documents are stored in a locked cabinet with access restricted to authorised employees only.

Sensitive project data such as plans of buildings are stored in a locked room. Access is restricted to authorised employees only.

4.3 Personal (HR) Data

Personal data required for HR purposes is processed by the Company in order to comply with employment law (HMRC requirement) and for, but not limited to, payroll (and associated pensions), career development (including appraisals), staff planning and disciplinary / grievance issues. Data will be retained whilst the person remains an employee and then for 36

months, unless longer retention is a legal requirement or we need the information for future projects. In the case of retention for future projects, only contact details will be kept. A full list of the personal data processed by the Company, together with the lawful reason for processing is available on request.

4.3.1 Special Categories of Personal Data (HR)

The Company will process special categories and criminal records data only when it is necessary and justified to enable the Company to meet its legal obligations and in particular to ensure adherence to health and safety legislation (which includes establishing a person's working capacity); vulnerable groups protection legislation, public interest (such as for equal opportunities monitoring purposes). Additional and explicit consent may be required for the Company to process this data. This data may also be needed in legal claims or to protect a person's vital interests.

4.4 Sensitive Project Data

Sensitive information relating to projects (past & current) is necessary for site access, planning and quoting / estimating. This information is required by the Company as a necessary part of the work being carried out within a specific project. The information will include, but not limited to, the contact details of the external parties (which may include additional linked parties), access details and plans of the site(s) within the project.

4.5 Accuracy of Personal Data and Sensitive Personal Data

The Company will review all personal data regularly to ensure that it is accurate, relevant and up to date.

To ensure the Company's files are accurate and up to date, and so that the Company is able to contact staff or, in the case of an emergency, another designated person, the Company must be notified as soon as possible of any change in personal details (e.g. change of name, address, telephone number, loss of driving licence where relevant, next of kin details, etc.).

4.6 Accuracy of Sensitive Project Data

It is the responsibility of the employees working on a specific project to ensure that the details are accurate and up to date.

4.7 Data Breaches

Under the Data Protection Act 2018 the Company must record all data breaches regardless of their effect and follow the Data Breach Procedure.

If we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, we will complete our Data Breach Form and follow our Data Breach Procedure. Dependant on the seriousness of the breach, we will also report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about the likely consequences of the breach and the mitigation masures we have taken.

4.8 Subject Access Requests

The Company provides a system for people (called data subjects) to ask what personal information is retained on them. To make a subject access request, a request should be sent to the Company. In some cases, the Company may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require. This applies to both personal data and sensitive personal data.

We will normally respond to a request within one month from the date we receive it. In some cases, such as where the Company processes large amounts of the individual's data, we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

In response to a request, the Company will advise the data subject:

- whether or not your data is processed and if so why; the categories of personal data concerned and the source of the data if it is not collected directly from you;
- to whom your data may be disclosed, including any recipients located outside the European Economic Area (EEA) and the safeguards that apply to any such transfers;
- for how long your personal data is stored or how that period is decided;
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the Company has failed to comply with your data protection rights; and/or
- whether or not the Company carries out any automated decision-making and the logic involved in such decision-making.

The Company will also provide a copy of the personal data undergoing processing. This will normally be in electronic form if the request was made electronically, unless otherwise requested.

5 EMPLOYEE RESPONSIBILITIES

All employees (see 3.2 for definition) are responsible for helping the Company keep personal data accurate and up to date. It is the employee's responsibility to advise the Company if personal data provided to the Company changes, for example, if there is a change to bank details or address.

Where an employee has access to the personal data of other employees, customers or clients in the course of their employment, the Company relies on the employee to help meet its data protection obligations.

The employee is required:

- to access only data that they have authority to access and only for authorised purposes;

- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, see 4.2.1 and the Company's IT Policy);
- not to remove personal data or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures, see 4.2.1 and the Company's IT Policy); and
- not to store personal data on local drives or on personal devices that are used for work purposes, see 4.2.1 and the Company's IT Policy.

Failure to observe these requirements may amount to a disciplinary offence which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to your dismissal without notice.

Adrian Crowe

Date: February 2021

Review Date: February 2022