DATA PROTECTION (GDPR) POLICY

1. INTRODUCTION TO DATA PROTECTION POLICY

Moreable Ltd collects and uses relevant personal data regarding customers, visitors, staff and other individuals who come into contact with the company. This information is gathered in order to enable it to provide equipment and to deliver services and its other associated functions, including complying with its statutory obligations.

We shall take all reasonable steps to hold and process this data only in accordance with this policy.

2. DEFINITIONS

“Processing” means anything done to personal data such as collecting, recording, organising, structuring, holding/storing, adapting, altering, retrieving, using, disseminating/disclosing, erasing, destroying or otherwise using data. Processing can be automated or manual.

“Customers” may include current, past or prospective customers.

“Staff” may include current, past or prospective staff.

“Data subject” means the identified or identifiable individual who is the subject of personal data or the person to whom the information is being held and relates to.

“Personal data or personal information” means any data or information which relates to a living individual who can be identified. This may include the individual’s – name (including initials), identification number, location data, and online identifiers such as usernames. It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identify. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

“Data Controller” means the person or organisation that determines the purpose and the means of processing of personal data.

“Data Processor” means a person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

“Personal Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3. PRINCIPLES, AIMS AND OBJECTIVES

This policy is intended to ensure that all personal data/information collected about customers, staff, visitors and other individuals is collected, stored and used/processed in

accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018).

The Policy applies to any personal information or data regardless of the way that it is held, i.e. in paper files or held electronically.

4. LEGISLATION AND GUIDANCE

This Policy meets the requirements of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's Code of Practice for subject access requests.

.

5. THE DATA CONTROLLER

Moreable Ltd processes personal data relating to customers, visitors, staff and other individuals and is therefore a data controller.

6. THE DATA PROTECTION OFFICER

The Data Protection Officer (DPO) is the first point of contact for individuals whose data Moreable Ltd processes and for the ICO. Moreable Ltd.'s DPO is Mrs Sandra Davison and is contactable at info@moreableltd.co.uk or by telephone 01869 221711

7. DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that Moreable Ltd must comply with. The principles say that personal data must be:

1. Processed fairly and lawfully and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary to fulfil the purpose for which it is processed
4. Accurate and kept up to date
5. Not kept longer than necessary for the purposes for which it is collected
6. Processed in accordance with the data subject's rights
7. Processed in a way that ensures it is appropriately secure

This Policy sets out how Moreable Ltd aims to comply with these principles.

8. COLLECTING PERSONAL DATA

8.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 "lawful bases" (legal reasons) to do so under data protection law.

• The data needs to be processed so that Moreable Ltd can fulfil a contract with the individual, or the individual has asked the company to take specific steps before entering into a contract;

• The data needs to be processed so that Moreable Ltd can comply with a legal obligation;
• The data needs to be processed to ensure the vital interests of the individual,

e.g. to protect someone's life;
• The data needs to be processed for the legitimate interests of Moreable Ltd or a third party (provided the individual's rights and freedoms are not overridden);
• The individual (or their carer where appropriate) has freely given clear consent.
For special categories of personal data, we will also meet one of the special categories conditions for processing which are set out in the GDPR and DPA 2018.
If we offer online services to customers, such as an online portal, we intend to rely on consent as a basis for processing.
Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

8.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

9. SHARING PERSONAL DATA

9.1 Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

• There is an issue with a customer, visitor or other individual that puts the safety of our staff at risk.

• We need to liaise with other agencies – we will seek consent as necessary before doing this:

• Our suppliers or contractors need data to enable us to provide services to our customers. When doing this, we will:

• Only appoint suppliers or contractors which can provide sufficient guarantees that they will comply with data protection law.

• Establish data sharing agreements with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

• Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

Contact details such as name, address and telephone number will be provided to our sub-contractors where customers require and have agreed to services from them and to our suppliers for goods delivery purposes only.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

• The prevention and detection of crime and/or fraud

• The apprehension or prosecution of offenders
• The assessment or collection of tax owed to HMRC
• In connection with legal proceedings
• Where the disclosure is required to satisfy our safeguarding obligations
• Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them respond to an emergency situation that affects any of our customers or staff.

Where we transfer personal data to a country or territory outside the EU, we will do so in accordance with data protection law.

9.2 Sharing third party personal data

If you give us information about another person, you confirm that the other person has appointed you to act on their behalf and agreed that you:

- Shall consent on their behalf to the processing of their personal data
- Shall receive any data protection notices on their behalf
- Consent on their behalf to the transfer of their personal data abroad

10. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Moreable Ltd holds about them. This includes:

• Confirmation that their personal data is being processed

• Access to a copy of the data

• The purposes of the data processing

• The categories of personal data concerned

• Who the data has been, or will be, shared with

• How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

• The source of the data, if not the individual

• Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO (see section 6). They should include:

• Name of individual

• Correspondence address

• Contact number and email address

• Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

10.2 Responding to subject access requests

When responding to requests, we:

• May ask the individual to provide 2 forms of identification

• May contact the individual via phone to confirm the request was made

• Will respond without delay and within 1 month of receipt of the request

• Will provide the information free of charge

• May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

• Might cause serious harm to the physical or mental health of the customer or another individual

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see

section 8), individuals also have the right to:

• Withdraw their consent to processing at any time

• Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)

• Prevent use of their personal data for direct marketing

• Challenge processing which has been justified on the basis of public interest

• Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

• Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)

• Prevent processing that is likely to cause damage or distress

• Be notified of a data breach in certain circumstances

• Make a complaint to the ICO

• Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all

of our data processing activities, including:

• Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

• Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 7)

• Completing privacy/data impact assessments where Moreable Ltd.'s processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

• Integrating data protection into internal documents including this policy, any related policies and privacy notices

• Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

• Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

• Maintaining records of our processing activities, including:

o For the benefit of data subjects, making available the name and contact details of our company and the DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

o For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any thirdparty recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

12. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks, pinned to notice/display boards, or left anywhere else where there is general access
- Where hard copy personal information needs to be taken off site, staff must sign it in and out from the company's office
- Passwords that are at least 8 characters long containing letters and numbers are used to access company computer, laptops and other electronic devices
- Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff who store personal information on their personal devices are expected to follow the same security procedures as for company-owned equipment
- User account access is controlled by a unique user name and password
- All data is stored on secure servers
- Payment details are encrypted using SSL

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 9)

13. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely.

Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

We may also use a third party to safely dispose of records on the company's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14. PERSONAL DATA BREACHES

We will make all reasonable endeavours to ensure that there are no personal data breaches.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a service industry context may include, but are not limited to:

• A non-anonymised dataset being published on the company's website (for example, a list of customers with names, addresses etc.

• The theft of a company laptop containing non-encrypted personal data about customers and staff

Author: J Davison

Date Reviewed: October 2024

Next Review Date: October 2027