

# Microcare Technologies Ltd

## Data Protection Policy

### 1. Introduction

This Policy sets out the obligations of Microcare Technologies Ltd, a company registered in England & Wales under number 08089449, whose registered office is at Stoke House, Church Road, Ashford, Kent, TN23 1RD (“the Company”) regarding data protection and the rights of its customers (“data subjects”) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one 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.

This Policy sets the Company’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed always by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

### 2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

- 2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- 2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.
- 2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- 2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- 2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to

implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of the data subject.

- 2.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

### **3. Data Security - Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- 3.1 All emails containing personal data must be encrypted All emails containing personal data must be marked “confidential”;
- 3.2 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- 3.3 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- 3.4 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- 3.5 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- 3.6 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient;
- 3.7 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

### **4. Data Security - Storage**

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- 4.1 All electronic copies of personal data should be stored securely;
- 4.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- 4.3 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise;
- 4.4 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been

taken).

## **5. Data Security - Disposal**

The Company shall ensure that when any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

## **6. Data Security - Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- 6.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested and approved;
- 6.2 Personal data must be handled with care always and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- 6.3 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the user must lock the computer and screen before leaving it.

## **7. Data Security - IT Security**

The Company shall ensure that the following measures are taken with respect to IT and information security:

- 7.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;
- 7.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;
- 7.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing all security-related updates after the updates are made available by the publisher or manufacturer or as soon as reasonably and practically possible, unless there are valid technical reasons not to do so.

## **8. Organisational Measures**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- 8.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy;
- 8.2 Only employees, agents, sub-contractors, or other parties working on behalf of

the Company that need access to, and use of, personal data to carry out their assigned duties correctly shall have access to personal data held by the Company;

- 8.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- 8.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- 8.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- 8.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- 8.7 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- 8.8 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR;
- 8.9 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that all their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR;
- 8.10 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.