DATA PROTECTION POLICY

Issue Date:28 May 2025
Next Review Date: 18 May 2026
Issued by: Nathan Oliver (CISO)
Version: 3.0

Table of Contents

1. Introduction

Microminder Cyber Security needs to gather and use certain information about individuals. This can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how data (including personal identifiable data) must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

- **Policy Aim**

This data protection policy ensures that Microminder Cyber Security:

- Complies with data protection law and follow good practice
- Protects the rights of team members, customers and partners
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach

2. Data Protection Law

- The Data Protection Act 2018 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether the data is stored electronically, on paper or other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
- In addition to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, Microminder Cyber Security complies with international data protection laws applicable in jurisdictions in which it operates. These include:
    - UAE Federal Decree Law No. 45 of 2021 (Personal Data Protection Law – UAE PDPL), enforced by the UAE Data Office.
    - Saudi Arabia's Personal Data Protection Law (PDPL), issued under Royal Decree M/19, and enforced by the Saudi Data and Artificial Intelligence Authority (SDAIA).

Our data protection practices reflect local regulatory requirements in the UK, UAE, and KSA, and the organisation implements adequate safeguards and controls in cross-border data transfers, contractual clauses, and data subject rights management in accordance with each jurisdiction

- The UK General Data Protection Regulation is underpinned by six important principles which say that personal data must be:
    - processed lawfully, fairly and in a transparent manner in relation to individuals;
    - 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 considered to be incompatible with the initial purposes;
    - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
    - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
    - 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; 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 the implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals; and
    - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. People, Risks and Responsibilities

• Policy Scope

This policy applies to:

- Unit 8a Wadsworth Rd, Perivale, Greenford UB6 7JD; and any other location where any work pertaining to Microminder Cyber Security is undertaken.
- All team members and volunteers of Microminder Cyber Security.
- All contractors, suppliers and other people working with or on behalf of Microminder Cyber Security.
- It applies to all data that the company holds relating to identifiable individuals.

• Data Protection Risks

This policy helps to protect Microminder Cyber Security from data security risks, including:

- **Breaches of confidentiality -** information being given out inappropriately or accidentally.
- **Failing to offer choice -** all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage –** Microminder Cyber Security would suffer if malicious threat actors gained access to sensitive data.

• Responsibilities

Everyone who works for or with Microminder Cyber Security has responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The CISO is responsible for:

- Keeping the board updated about data protection responsibilities, risk and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from team members and anyone else covered by this policy.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other team members to ensure marketing initiatives abide by the data protection principles.

The CISO is responsible for:

- Responding to subject access requests (SARs) and ensuring data subjects can exercise their rights effectively under GDPR, PDPL (UAE and KSA), and other applicable laws.
- Informing and communicating with the Information Commissioner's Office (ICO) where necessary.

4. Policy Statement

5. Data Storage

These rules describe how and where data should be safely stored and processed.

- Access to data should be restricted to only those who need it for their work, via the principle of least privilege permissions.
- Data should not be shared informally.
- When access to CONFIDENTIAL or RESTRICTED data is required, team members can request it from their line manager. If the line manager does not have authorisation to access the data, it should be followed up with their respective line manager.
- Microminder Cyber Security will provide training to all employees to help them understand their responsibilities when handling data.
- All software the company provides or recommends is correctly licenced. This applies to software that has access to company or customer data.
- Passwords should never be shared between users.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required (in the case of Lidl GB, after two years of sending the report out}, it must be securely deleted or disposed of.
- Data should only be stored on paper when essential or for legal purposes. It should be standard practise to only store data electronically (digital data).
- Data printouts should be shredded or disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. Some ways of achieving this are listed below:
- Data must be protected by strong passwords that are changed regularly and never shared between team members.
- If data is stored on removable media (like a CD or DVD), its storage must be authorised by the CISO and all personnel use only approved storage media. These media (such as flash drives) must be kept locked securely when not in use and protected by a strong password and encryption when at rest.
- Data should only be stored on designated drivers and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- All sensitive data such as customer data and personal identifiable information must be encrypted-at-rest using AES-256 or a similar good practice encryption algorithm.
- All sensitive data must be encrypted-in-transit during handling using TLS, SFTP, SSH or similar.
- All team members devices should use full disk encryption.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard for backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones unless you have the full suite of security protection installed and configured.
- All servers and computers containing data should be protected by approved security software and a firewall.

6. Data Use

Personal data is of no value to Microminder Cyber Security unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

When working with company and personal data, employees should **ensure the screens of their computers are always locked** when left unattended.

Personal and company data **must not be shared informally**, such as by email, as this form of communication is not secure unless encryption is in place and the intended recipient is trusted and correct.

Microminder Cyber Security may transfer personal data outside the UK, UAE, or KSA to service providers or business partners. Such transfers are subject to strict safeguards, including Standard Contractual Clauses (SCCs), data transfer impact assessments (DTIAs), or other legally approved mechanisms. We ensure that equivalent protection is maintained regardless of the destination of the data in accordance with the applicable jurisdiction's laws (e.g., UK GDPR, UAE PDPL, KSA PDPL).

Team members should **not save copies of personal data to their computers**. Always access and update the central copy of any data.

7. Data Accuracy

The law requires Microminder Cyber Security to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Microminder Cyber Security should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be **held in as few places necessary**. Team members should not create any unnecessary additional data sets.

Team members **should take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call, if personal information is held for that customer.

Microminder Cyber Security will make it **easy for data subjects to update the information** Microminder Cyber Security holds about them.

Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Data retention is governed by Microminder's formal data retention schedule, which defines minimum and maximum retention periods for all data categories based on legal, operational, and contractual obligations. Data no longer required is securely deleted or anonymised in accordance with ISO/IEC 27001 Clause A.5.32 and NCA ECC-5.

8. Subject Access Requests

- All individuals who are the subject of personal data held by Microminder Cyber Security are entitled to:
    - Ask **what information** the company holds about them and why.
    - Ask **how to gain access**.
    - Be informed about **how to keep it up to date**.
    - Be **informed about how the company is meeting its data protection obligations**.
- If an individual contacts the company requesting this information, this is called a subject access request.
- Subject access requests from individuals should be made by email addressed to the data controller. The data controller can supply a standard request form, although individuals do not have to use this. The data controller will aim to provide the relevant data within the time permitted by the regulations.
- The data controller will always verify the identity of anyone making a subject access request before handing over any information.
- If a person exercises any of their rights under data protection law, Microminder Cyber Security shall ensure that a response will be given no later than one calendar month from the day the request has been received.

9. Disclosing Data For Other Reasons

- In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Microminder Cyber Security is also required to disclose personal data to enforce Microminder Cyber Security's EULA or to protect the property, rights or safety of Microminder Cyber Security,

users of Microminder Cyber Security's services or others. In such a case, information may be exchanged with third-party companies or organisations to prevent fraud or reduce credit risk.

- Under these circumstances, Microminder Cyber Security will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

10. Disclosing Data To Third Parties

Disclosure of personal data (including, without limitation, Client Data) to third parties will only occur if:

- Microminder Cyber Security sells or purchases any business or assets. In such a case, Microminder Cyber Security may authorise the disclosure of personal data to prospective sellers or buyers of such business or assets.
- All or the substantial majority of Microminder Cyber Security is sold to a third party. In such a case, personal data may be one of the transferred assets.

11. Data Breach Management

Microminder Cyber Security has a defined incident response process for identifying, managing, and reporting data breaches. Our breach response process is aligned with ISO/IEC 27001:2022 Clause A.5.25 and the applicable legal obligations of each jurisdiction in which we operate. This includes:

- Detecting and containing personal data breaches;
- Notifying the Information Commissioner's Office (ICO) in the UK, the UAE Data Office, or SDAIA in KSA, where required, without undue delay and within 72 hours of becoming aware of a notifiable breach;
- Informing affected individuals if there is a high risk to their rights and freedoms;
- Documenting all incidents, decisions, actions taken, and lessons learned

12. Further Information

Further information and advice on this policy can be obtained from Nathan Oliver (CISO). – contact Nathan.oliver@microminderc s.com

Comments and suggestions to improve security are always welcome.

13. Policy Review and Governance

This policy is reviewed annually or in response to significant changes in legislation, business operations, or technology. The review is led by the CISO and approved by the Board of Directors.

Changes will be communicated internally to all staff and reflected in the version control of the document. If updates materially affect how personal data is handled, stakeholders and clients will be informed as required.