Data Protection Policy

Version: 1.7

Date: 1/11/2026

Approved by:



Jamal Kubeer
General Manager

Contents

Introduction 3
Why this policy exists 3
Data protection law 3
Policy scope 3
Data protection risks 4
Responsibilities 4
General staff guidelines 5
Data Classification 5
Classification Levels 6
Data storage 7
Data use 8
Archiving / removal 8
Data accuracy 9
Disclosing data for other reasons 9
Providing information 9

Introduction

Automated Services Network Company (eNet) needs to gather and use certain information about individuals.

These 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 this personal data must be collected, handled, and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures eNet:

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

Data protection law

The Data Protection Law describes how organisations — including eNet— must collect, handle, and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant, and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy scope

This policy applies to:

- The head office of eNet
- All staff and volunteers of eNet

- All contractors, suppliers and other people working on behalf of eNet

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Law. This can include:

- Names of individuals
- Identity information
- Addresses
- Email addresses
- Telephone numbers
- ...plus, any other information relating to individuals

Data protection risks

This policy helps to protect eNet from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with eNet has some 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.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that eNet meets its legal obligations.

- The **General Manager,** is responsible for:

    - Keeping the board updated about data protection responsibilities, risks, 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 staff 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.

- The **IT Administrators and Support,** is responsible for:
    - 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.
    - Data Protection policy and implementation

- The **Business Development Manager,** is responsible for:
    - 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 staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **eNet will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used,** and they should never be shared.
- 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, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Classification

Classifying data into separate categories helps in better decisions making, regarding data access and processing in line with the data classification levels mentioned in

this policy, which contributes in helping company entities to take all necessary measures to enhance the security and protection of their data and the personal data they have of the individuals, in a consistent manner with the requirements and institutions plans, laws and regulations applicable.

Classification Levels

1. **Public**
   Public data is information that may be disclosed to any person regardless of their affiliation with the Company. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside the Company community and no steps need be taken to prevent its distribution.

2. **Internal**
   Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of the Company without the permission of the person or group that created the data. It is the responsibility of the data owner to designate information as Internal where appropriate. If you have questions about whether information is Internal or how to treat Internal data, you should talk to your manager or department head.

3. **Confidential**
   Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or the business of the Company. This classification also includes data that the Company is required to keep confidential, either by law or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

4. **Restricted Use**
   Restricted Use data includes any information that Company has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the Company to notify the affected individual or authorities. In some cases, modification of the data would require informing the affected individual.
   The Company's obligations will depend on the data and the relevant contract or laws. The Minimum-Security Standards sets a baseline for all Restricted

Use data. Systems and processes protecting the following types of data need to meet that baseline:

- Personally Identifiable Information (PII) covered under law, including an individual's name plus the individual's Civil Id, driver's license number, or a financial account number.
- Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored.
- Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens.
- "Criminal Background Data" that might be collected as part of an application form or a background check.

Restricted Use data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of Restricted Use data must be reported to the General Manager of the company.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When sensitive data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to sensitive data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper, and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When sensitive data is **stored electronically**, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Sensitive Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used. Stored Data should be encrypted by secret encryption 'key', which is generated or protected by a user-supplied password or passphrase.
- Sensitive Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Sensitive Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Sensitive Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing sensitive data should be protected by **approved security software and a firewall** when sensitive data is transferred by internet or Emails, approval

Data use

Personal data is of no value to eNet 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 personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Archiving / removal

By Law eNet will keep personal data archived for **a total of 10 years**. eNet shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

The archiving policy shall consider what data should/must be retained, for how long, and why.

Data accuracy

The law requires eNet 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 eNet 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 as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- eNet will make it **easy for data subjects to update the information** eNet holds about them. For instance, via the company website.
- 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.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Disclosing data for other reasons

In certain circumstances, the Data Protection Law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, eNet 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.

Providing information

eNet aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.