Introduction

Mardon LTD needs to collect and use certain types of information about Individuals. These can include customers, suppliers, business contacts, employees and other people the company 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 Mardon LTD:

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

Data protection law

The EU General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, describes how organisations, including Mardon LTD, 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 GDPR is underpinned by six important principles:

1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality

In addition to those principals the personal data must 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 Mardon LTD
- All branches of Mardon LTD
- All employees of Mardon LTD
- All contractors, and other people working on behalf of Mardon LTD

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

- Names of individuals
- Postal addresses
- Email addresses. Any e-mails with individual's name on it for instance paul.smith@company.com.
- Telephone numbers
- Passport numbers
- NI numbers
- Bank account numbers

Data protection risks

This policy helps to protect Mardon LTD, staff, customers, suppliers and other business contacts from some very real data security risks, including:

- Personal data breaches. 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 Mardon LTD 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, data protection principles and current legislation.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Mardon LTD meets its legal obligations.
- The Accounts Manager – is responsible for:
    - Checking and approving any contracts or agreements with third parties that process personal data Mardon LTD passes to them. For example Moore and Smalley charted accountants.
    - Make sure all employees record files stored securely and that only authorised persons have access to them.
- The IT Manager – is responsible for:
    - Ensuring all systems and company provided 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.
    - 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 relevant third parties covered by this policy.
    - Dealing with requests from individuals to see the data Mardon LTD holds about them (also called ‘subject access requests’).
- The Directors are responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

All 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.
- Mardon LTD can 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 utilised 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 if they are unsure about any aspect of data protection.

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.

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

These guidelines also apply to data that is usually stored electronically but has been printed out for valid reasons:

- 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 data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- 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.
- Removable USB pen drives will need to be encrypted and password protected prior to being used to store company data, especially if the device is to be taken off company premises. Third party contractors will be expected to use similar encryption / protection method when attempting to transport authorised company data.
- Imported removeable media will not be opened / used without scanning the contents first (in some cases sandboxing technologies will put in place prior to scanning)
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Mardon LTD 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 and other electronic device are always locked when left unattended, especially when out of company premises.
- 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.

Data accuracy

The law requires Mardon LTD to take reasonable steps to ensure data is kept accurate and up to date.

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
- Data should be updated when inaccuracies are discovered. For instance, if individuals can no longer be reached on their stored telephone number, it should be removed from the database or updated if there is a case for it.

Subject access requests

All individuals who are the subject of personal data held by Mardon LTD are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If some individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email or in person to the IT Manager or one of the Directors.

The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

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

Under these circumstances, Mardon LTD will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Directors and from the company's legal advisers where necessary.

Providing information

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

- How the data is being used, stored (retention and security of)
- How to exercise their rights

Personal Data breach

What is a personal data breach

A personal data breach refers to a breach of security that can lead to the destruction, loss, alteration and unauthorised disclosure of, or access to, personal data. So, a breach is more than just losing personal data.

How we report a breach

A breach will be reported to the relevant supervisory authority within 72 hours Mardon LTD became aware of it (ICO help line - 0303 123 1113).

What information should be included in a notification

The information that should be included in a notification of a data breach is:

- The type of personal data breach, including
- The type and estimated number of individuals affected
- The type and estimated number of personal data records concerned
- The name and contact details of a point of contact where further information can be obtained.
- The possible outcomes of the personal data breach
- A list of measures taken or being taken to deal with the breach and appropriate measures taken to mitigate any adverse effects.

When do the individuals affected have to be notified

If a breach is likely to result in a high risk to the rights and freedoms of individuals, those affected will be notified directly.

This is when the need to notify an individual outweighs the need to notify the relevant supervisory authority.