

Lawnswood Fencing Ltd

General Data Protection Policy

Policy Date	25.05.2018
Written by	Julie Smith
Position	Health & Safety Officer
Signature	
Last review	5.06 2023

Data Protection Policy

Context and overview

Key Details

- Policy prepared by: Julie Smith
- Approved on: 09.05.18
- Policy became operational on: 25.05.18
- Next review date: 01.06.24

Introduction

Lawnswood Fencing Ltd is fully committed to full compliance with the requirements of the General Data Protection Regulation. Lawnswood will therefore follow procedures which aim to ensure that all employees, contractors, consultants, partners who have access to any personal data held by or on behalf of Lawnswood are fully aware of and abide by their duties under the General Data Protection Regulation.

Lawnswood Fencing Ltd needs to collect and use information about people with whom it works in order to operate and carry out its functions. These may include members of the public, current, past, and prospective employees, clients and customers and suppliers. In addition, Lawnswood may be required by law to collect and use information. This personal information must be handled and dealt with properly however it is collected, recorded, and used whether it on paper, in computer records or recorded by other means.

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

Why this policy exists.

This data protection policy ensures that Lawnswood Fencing Ltd:

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

Data Protection Law

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998, it is designed to harmonize data privacy laws across Europe, to protect and empower all EU Citizens data privacy and to reshape the way organizations across the region approach data privacy.

These rules must 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 General Data Protection Regulations are 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 is necessary
6. Be processed in accordance with the rights of the data subjects
7. Be protected in appropriate ways- kept safe and secure
8. Not be transferred outside the European Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks, and responsibilities

Policy scope

This policy applies to:

- The Directors of Lawnswood Fencing Ltd
- All employees of Lawnswood Fencing Ltd
- All contractors, suppliers, and partners of Lawnswood Fencing Ltd

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to an individual

Data protection risks

This policy helps to protect Lawnswood Fencing Ltd from data security risks including.

- **Breaches in 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, and have the right to be forgotten
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data

Responsibilities

Everyone who works for or with Lawnswood Fencing Ltd has some responsibility for ensuring data is collected, stored, and handled appropriately.

Each department or 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 responsibilities:

- The **Directors** are ultimately responsible for ensuring that Lawnswood Fencing meets all its legal obligations.
- The **Head of Data Protection**, Director Helen Foster is responsible for:
 - Keeping updated about data protection responsibilities, risks and issues
 - Handling data protection questions from staff and anyone else covered by this policy
 - Dealing with requests from individuals to see the data Lawnswood Fencing holds about them (also called subject access request)
 - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
 - 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
 - Addressing data protection issues on outlets such as sales and marketing products and social media
 - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- The **Data Protection Team**: Helen Foster and Julie Smith are responsible for:
 - Reviewing all data protection procedures and related policies, in line with an agreed schedule
 - Arranging data protection training and advice for people covered by this policy
 - 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
 - Where necessary, working with other employees to ensure marketing initiatives abide by data protection principles

General employee 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 the Data Protection Team

- Lawnswood Fencing will provide information and training to 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.
- Employees should request help from the Data Protection Team 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 data safety can be directed to the Data Protection Team.

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

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

- When not required the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper printouts are not left where unauthorised people could see them, such as on a printer
- Data printouts when no longer required should be disposed of securely in the container provided by a confidential waste disposal company or at least shredded

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 CD, DVD or USB), these should be kept locked away securely when not being used
- 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
- 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 smartphones
- 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 Lawnswood Fencing 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 inappropriate use, 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 must not be shared informally
- Permission must be sought before use of photographic material and reference to individuals may be published
- Employees should not have personal data on their own computers, tablets, or mobile phones

Further information on data use is stated in the **Data Protection Procedures**

Data accuracy

The law requires Lawnswood Fencing Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that personal data is accurate, the greater the effort Lawnswood Fencing Ltd 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. Employees 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
- Data should be updated as inaccuracies are discovered. For example, if a customer can no longer be reached on their stored number, then it should be removed from the data base

Subject access requests

All individuals who are subject of personal data held by Lawnswood Fencing 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 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 Head of Data Protection at helen@lawnswoodfencing.co.uk, however it is noted that some individuals may wish to make such requests in person.

The Head of Data Protection will aim to provide relevant information within 14 days.

The Head of Data Protection will always verify the identity of anyone making a subject access request before handing over information.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulations:

Allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Lawnswood Fencing Ltd will disclose requested data. However, the Head of Data Protection will ensure the request is legitimate.

Providing information

Lawnswood Fencing Ltd 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 Notice setting out how data relating to individuals is used by the company.