General Data Protection Regulation Policy

Context and overview

Introduction

Elder Engineering (Herts) Ltd 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 will be collected, handled and stored to meet the company's GDPR standards.

Why this policy exists

This GDPR policy ensures Elder Engineering (Herts) Ltd:

- Complies with GDPR 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

GDPR is how organisations — including Elder Engineering (Herts) 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.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Elder Engineering (Herts) Ltd
- All staff of Elder Engineering (Herts) Ltd
- All contractors, suppliers and other people working on behalf of Elder Engineering (Herts) Ltd

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

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect Elder Engineering (Herts) Ltd 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 Elder Engineering (Herts) Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each member of staff that handles personal data must ensure that it is handled and processed in line with this policy and GDPR principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Elder Engineering (Herts) Ltd meets GDPR obligations.
- The Data Protection Officer**,** is responsible for:
    - Keeping the board updated about GDPR responsibilities, risks and issues.
    - Reviewing all GDPR procedures and related policies, in line with an agreed schedule.
    - Arranging GDPR training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Elder Engineering (Herts) Ltd holds about them.
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- Approving any GDPR statements attached to communications such as emails and letters.

- The IT support supplier, 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.

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.
- Elder Engineering (Herts) Ltd 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 storage

Data stored on paper, 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:

- 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, these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers.
- 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 Elder Engineering (Herts) Ltd unless it is used for..

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by a

controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Data accuracy

GDPR requires Elder Engineering (Herts) 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. For instance, by confirming a customer's details when they call.
- Elder Engineering (Herts) Ltd will make it easy for data subjects to update the information Elder Engineering (Herts) Ltd 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.

Subject access requests

All individuals who are the subject of personal data held by Elder Engineering (Herts) 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 data controller at accounts@elderengineering.co.uk.

The data controller will aim to provide the relevant data within 30 days unless the data requested is complex or onerous, in which case we will extend the deadline by up to 2 months.

We will not normally charge for this unless the request is manifestly unfounded or excessive, in which case we may charge a reasonable administration fee.

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

Under these circumstances, Elder Engineering (Herts) Ltd 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 and will only provide data relevant to the request.