GDPR & Data Protection Policy

Statement

E&M Lifts Ltd (the "Company") will need to gather information relating to individuals, customers, suppliers, business contacts, employees and other people who may need to be contacted to enable the company to carry out its business activities.

As a company we need to gather information for various reasons such as providing a service, employment or contractual obligations.

This policy sets out the company's commitment to comply with law, good practice relating to those companies or individuals whose data we hold. It is in place to ensure that the rights of our staff, customers and partners are protected and provides information on how we store and process data. It also serves to protect the company from the risks associated with a data breach.

The company takes our responsibilities in relation to data protection seriously and are registered with the Information Commissioners Office (ICO).

Data Protection Laws

The Data Protection Act 2018 is the UK's primary piece of legislation which controls how personal information is used by organisation, businesses and government and is the UK's implementation of the General Data Protection Regulations. It provides instruction and guidance on how we as a company collect, handle and store personal information regardless of whether the data is stored electronically or on paper.

The eight key principals of the Data Protection Act required that all personal data must:

1. Be processed fairly and lawfully
2. Be obtain only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not beheld for any longer than necessary
6. Processed in accordance with the rights of the data subject
7. Be protected in appropriate ways
8. Not be transferred externally, unless absolutely necessary and subject to the external body also providing the same level of protection.

People, Risk and Responsibilities

People

This policy applies to the head offices and any associated business locations, employees, consultants, volunteers, contractors, suppliers or any other party who is provided access to the company data.

It applies to all data that the company may hold relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include, but is not limited to:

- Individuals Names
- Addresses
- Emails
- Phone Numbers
- Identification Documentation

Risks

This policy is in place to protect the individuals but also the company from the reality of data security risk. These risks could include, but are not limited to:

- Breach of confidentiality by issuing out individuals' information inappropriately
- Failing to offer individuals a choice on how the company uses their data
- Reputational damage as a result of a hacker successfully gaining access to sensitive data

Responsibilities

Each individual within the company has a responsibility for ensuring data that is collected is stored and handled appropriately ensuring it is done so in line with this policy and the data protection principals.

There are however certain key members who will have specific responsibilities.

The **Managing Director** has ultimate responsibility for ensuring that the company meets its legal obligations and ensuring that appropriate measures and procedures are in place to reduce the risk as far as is possible.

Where appointed, the **Data Protection Officer (DPO)** is responsible for ensuring that the Managing Director remains updated about the data protection responsibilities, risks and issues relating specifically to data protection.

The company Directors will support the DPO by ensuring that all policies and procedures relating to data protection are reviewed and updated in line with current legislative requirements and will arrange for all employees to complete the necessary GDPR training appropriate to their role within the company. In

addition, they will ensure that all data protection related questions from staff or other parties are dealt with in accordance with the requirements set out within this policy. All requests from individuals to see the data that the company hold about them (also referred to as "subject access request") will be dealt with confidentially and accordance with the requirements set out by law.

The person responsible for all **Information Technology (IT)** is responsible for ensuring that all systems, services and equipment used for storing data meets the required security standards, for performing regular checks and scans on all hardware and software to ensure they are functioning properly.

The appointed marketing consultant is responsible for ensuring that any data protection statements attached to communications such as emails and letters are approved, addressing queries from journalists or media outlets like newspapers. Where necessary, when working with other employees to ensure marketing initiatives abode by data protection principals.

Opting out and Withdrawing Consent

The company will accept any request from an employee to opt out of their data being used in a particular way and acknowledges that even if consent is obtained it can be withdrawn.

The company will however, where required by law, retain data for a certain length of time, even though consent for using it has been withdrawn.

Guidelines for all Employees

Employees who need to access data to enable them to carry out their day-to-day tasks will be covered by this policy. Data MUST NOT be shared informally without the consent of the individual. Where access to confidential information is required this request must be directed to the employees Line Manager for approval.

All employees who are required to access subject data to perform their task must complete the GDPR training allocated to them to ensure that they fully understand the requirements as set out within the Act.

Employees must ensure that all precautions are taken to ensure that the data is kept secure by following the guidelines below:

- Strong passwords must be used and they should never be shared
- Personal data must not be shared either within the company or externally
- Data must be reviewed regularly and if found to be out of date or if no longer required it must be deleted
- Request support from line managers should they be unsure about any aspect of data protection

Storage of Data

There are clear guidelines on how to store data safely. If you are unsure please speak to your line manager or the appointed IT contact about where this should be. Below are some simple guidelines to follows.

Where data is on paper:

- This should be stored in a secure place that unauthorised personnel are not able to access
- When electronically stored but printed off for use to carry out your allocated tasks then this should be kept in a locked drawer or filing cabinet
- Do not leave documents containing personal information laying around for other to see
- When printing out electronic data ensure that you collect it promptly from the printers
- When the printed data is no longer required then it should be shredded

Electronic Data:

- Strong passwords must be used and changed regularly, do not share with others
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing system
- Servers containing personal data should be sited in a secure location away from the general office space
- Data should be backed up frequently and backups tested regularly
- Date should never be saved directly onto 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

Use of Data

The company will only hold personal data, which is needs to perform its daily functions. This has no monetary value to the company however, if personal data is accessed and used incorrectly this could result in a corruption or theft.

To reduce the risk of unauthorised access:

- Screens should always locked when you move away from your desk
- Data should not be shared informally, do not send by email as this form of communication can never be 100% safe
- Where possible encrypt date before transferring
- No personal data must be saved on an individual's personal computer.
- Access should only ever be by authorised personnel who have access to the central storage location

Accuracy of Data

To ensure compliance with the law the company require that all reasonable steps be taken to ensure that date is kept accurate and up to date and the level of security is appropriate for the data stored. Employees must ensure that they take all reasonable steps to ensure data is current.

Data must be held in as few locations as possible and the information held updated as soon as a change has been notified or identified. Inaccurate or out of date data should be permanently deleted, except whether the specific data is required to be stored for a period of time by law.

Subject Access Request

Any individuals who are the subject of data held by the company is referred to as a "subject". The subject is entitled to ask about the information the company holds about them, why it is being held, how access is gained and be informed about how it is kept up to date. They may also ask for evidence on how the company is meeting its data protection obligations.

Should an individual contact the company requesting access to the information held this is called a subject access request. All subject access requests must be made in writing to the company and must be provided with this information, free of charge, within 14 works days of receipt of the request, subject to the request not requiring excessive resource to action it. Prior to providing any information on an individual the identify of the subject must be verified.

Disclosing Data for Other Reasons

There are circumstances which allow disclosure of personal data without consent. The Act permits personal data to be made available to law enforcement agencies without the consent of the data subject. Under these circumstances the company will be required to disclose all data requested. The company must however ensure that the request is legitimate and if unsure seek legal advice prior to disclosure.

Review

This policy will be issued to all employees, on request from external interested parties and will be reviewed as required.

Signed and dated

06th January 2026

Robert Evans

Managing Director