General Data Protection Regulation Organisational Procedure

Introduction

This policy aims to set out the Company's policies and procedures in relation to the General Data Protection Regulations (GDPR) at an organisational level. As such, this policy outlines the Company's procedures relating to the obtaining, maintaining, processing and destroying of personal data.

Premier Electrics has a duty of care to ensure that all our practices are safe and compliant and protect personal data. Premier Electrics is committed to safety and our processes are designed to protect those whose personal information we hold. This policy also sets out how Premier Electrics aims to protect personal data and ensure that this is implemented across the breadth of employment activities.

The Premier Electrics holds personal data about its employees, clients, stakeholders and other individuals for a variety of documented business proposes. Premier Electrics complies with current data protection legislation when obtaining, maintaining and destroying personal data.

General Data Protection Guidance

The GDPR sets out principles regarding the use of personal data that set the framework upon which data processing activities are conducted. As such, all personal data must:

- Be processed lawfully, fairly and in a transparent manner
- Be collected for a specific, explicit and legitimate purpose and not further processed in a manner which is incompatible with that purpose
- Be adequate, relevant, and limited for what is necessary in relation to the purposes for which it is processed
- Be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased and rectified without delay whilst having regard to the purposes for which they are processed
- Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures

Premier Electrics must have relevant procedures in place in order to demonstrate accountability and compliance with each of the above principles which are set out in the General Data Protection Regulations.

Data Types

The GDPR legislation defines 'personal data' as information relating to an identified or identifiable natural person ("data subject") who can be identified directly or indirectly by reference to an identifier. This can be an identification number, a location number, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person. These are all examples of personal data, however this is not an exhaustive list. All personal data is carefully managed by the Company.

Sensitive data is defined, for data protection purposes as information concerning a data subject's racial or ethnical origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual orientation or criminal offences and convictions.

Types of Information Held

The purpose for which we obtain, maintain and destroy any personal information is for use solely for administrative and personnel management purposes; including but not limited to:

- Recruitment.
- Appraisals and performance management.
- Promotion.
- Training & career development.
- Pay and remuneration.
- Pension and insurances and other benefits.
- Tax, national insurance and other deductions from pay.
- Health and safety.
- Discipline and grievances.
- Review of our human resources policies.
- Correspondence with the Organisation and other information provided to the Organisation by other Organisations.

Organisational Procedures

Data Protection Officer (DPO) or Equivalent

As part of Premier Electrics' commitment to strictly adhere to data protection legislation, Premier Electrics has appointed a Data Protection Officer (DPO), or equivalent representative, who is responsible for overseeing the Company's strategies and implementation of data protection policies and procedures at an operational level. The Data Protection Officer (DPO), or equivalent representative, is an independent and accountable mechanism who will ensure data protection compliance.

The Data Protection Officer (DPO), or equivalent representative, is responsible for:

- Advising senior management and the Board of all data protection obligations, risks and concerns
- Regularly and consistently reviewing all data protecting procedures and policies so as to adhere to data protection legislation
- Being the Company's point of contact for all data protection queries from staff, senior management, board members and other Premier Electrics' stakeholders and the ICO
- Responding to all subject access requests from employees, clients and individuals, unless otherwise agreed
- The management of contracts or agreements with third party companies which hold or process Premier Electrics' personal data and ensuring that they adhere to data protection requirements

Organisational Responsibilities

At an organisational level, Premier Electrics is responsible for:

- Ensuring that appropriate resources are in place for which employees can undergo data protection training to ensure compliance within individual employee roles
- Ensuring that appropriate resources are in place for the storing, gathering, processing and transferring of personal data
- Regularly analysing and documenting the types of personal data that we hold
- Regularly checking and reviewing our procedures to ensure that they are fully compliant and all individual rights are being adhered to
- Identifying the lawful basis for which we as a Company process personal data
- Ensuring that consent procedures which are in place and compliant with current legislation
- Strategising and implementing procedures which identify, report and investigate any personal data breaches
- Ensuring that relevant procedures and resources are in place in which to store and delete data in a safe and secure manner
- Regularly assessing the risk to individual rights and freedoms should any of their personal data be compromised through a data breach

Privacy Notices

A privacy notice is a disclaimer which advises why personal data is being obtained and how this data will be maintained or destroyed. Privacy notices will be provided where necessary in a way that is concise, transparent, intelligible and easily accessible. They will be written in clear and plain language so that they are accessible and will be understood by all audiences; this is particularly true if they are aimed at children. Privacy notices will be provided free of charge and will be used where appropriate, as outlined within data protection legislation.

Data Retention and Data Destroying

Data will not be kept for longer than is necessary, as per the requirements of data protection legislation. Unrequired data will be destroyed as soon as reasonably practicable in a secure manner. Paper documentation will be shredded and electronic resources will be wiped using appropriate measures.

Data Security

As part of the organisations commitment to confidentiality, all data will be secure through the following procedures:

- Confidential paper records will be held in a locked filing cabinet, drawer or safe; Access will be restricted and will only be applicable to appropriate individuals.
- Confidential paper records will not be left unattended or in clear view in an area with general access.
- Electronic data will be encrypted or held securely in a password-protected area.
- Where data is held on a portable or removable storage device, the device will be kept in a secure manner when not in use.
- Memory sticks will not be used to hold personal data unled they are password protected and encrypted.
- All electronic devices used within the organisation will be password protected to protect information in case of theft. Where possible, remote blocking will be enabled in instances of theft.
- All members of staff will be provided with their own digital accounts and will have individual logins and passwords. Passwords will be changed on a regular basis, where appropriate.
- Emails or electronic communications which contain sensitive or confidential personal data will be password protected if there are unsecure servers between the sender and the recipient.
- Where the organisation uses autofill email addresses, the employee will be expected to take necessary steps to protect the content of the information and organisation's reputation.
- In instances where information which is considered personal or confidential is taken off the Company premises, the organisation expects employees to take every reasonable precaution to protect the data. Employees will take extra care to follow the same procedures for security (e.g. keeping devices under lock and key and not

leaving information unattended in a vehicle). The individual taking the data will take full responsibility for the security of the data.

- The physical security of the Company buildings or premises is reviewed on a regular basis. If there is an increased risk to security, extra measures will be implemented to secure data.

Sharing Agreements

Sharing agreements are contracts between parties which outline the obligations, responsibilities and liabilities in relation to the protection of data. Where appropriate, Premier Electrics will obtain signed sharing agreements with third parties in instances where personal data is shared. This sharing agreement is designed to ensure that third parties have sufficient safeguards in place, concerning the compliance of GDPR.

If your personal data is to be shared with a third party, you will be notified in advance.

Staff Training

Employees will receive adequate training on the requirements of the data protection processes upon commencement of their employment. Training will raise data protection awareness amongst staff and will help them understand their data protection obligations and responsibilities. Employees will be given the tools to ensure that personal data is protected and processed lawfully during the course of their employment. Should training updates or refreshers be required, this will be carried out without delay. Employees are required to complete all assigned data protection training as requested by the Company; all training undergone will be signed off by the employees and documented as appropriate.

Subject Access Request

Under the Freedom of Information Act (FOIA), which came into effect on 1 January 2005, you have the right to request official information, including information in unstructured systems. All information is covered by FOIA, irrespective of protective markings or format. Information in emails, miscellaneous collections of papers, registered paper and electronic files is all potentially disclosable.

The Data Protection Act 1998 (DPA) and Freedom of Information Act (FOIA) are inter-linked, with requests under the FOIA that involve personal data being subject to the rules of the DPA. This means that information about third parties will normally be exempt from disclosure under the FOIA, and requests for information about yourself will be dealt with under the DPA.

If you wish to access the personal data which we hold about you, you must make a request in writing to the Data Protection Officer (DPO) or equivalent. There will be no fee for making a subject access request, however in instances whereby requests are excessive and or repetitive, an administration fee may be applied.

We will respond to your request without delay and at latest, within one month of receiving the written request. If necessary, this timescale can be extended by a further two months if the request is complex. However, you will be contacted within one month of the receipt of the request and we will explain why an extension is necessary in this instance.

The Company will endeavour to provide the information in a commonly used electronic format. Some information may be exempt from subject access requests, in such instances, your Data Protection Officer (DPO) or equivalent will explain the reasons why this request will not be carried out.

Exemptions

Certain types of data are exempt from disclosure under the DPA. Most of it that is exempt relates to data pertaining to third parties, that is other identifiable individuals. For example, in instances where a document on your personnel file includes data relating to another individual(s), you may not have a right of access to that data, or any data that would serve to identify the individual(s) concerned.

Other examples of data that may be exempt from disclosure could be that relating to, for example, the prevention and detection of crime, the collection of tax or duty and national security.

Reporting Data Protection Breaches

It is our obligation to report breaches to the ICO where deemed appropriate. A breach within the organisation must be appropriately reported without delay.
In certain circumstances, it is our obligation to report breaches to the ICO (regulatory body) within 72 hours of becoming aware. This will be the responsibility of the DPO, or equivalent. All employees are obliged to report actual or potential breaches or compliance failures. This will allow Premier Electrics to:

- Carry out an appropriate investigation into the breach, near miss or failure and take necessary steps
- Keep a documented register of compliance failures and near misses in order to show accountability going forward. (We will keep a register of any and all breaches, regardless if they have been notified to the ICO)
- Inform the ICO of such breaches or failures, as deemed appropriate.

Any employee of the Company, who fails to notify Premier Electrics of a potential or actual breach but had knowledge of such a breach, is liable to face disciplinary action due to not following the correct Company reporting procedures.

Failure to Comply with the GDPR Guidelines

Premier Electric stakes its responsibility to protect personal data extremely seriously and as such organisational compliance to current data protection legislation is of the highest importance. Failure to comply with the Company's protection policies and procedures puts both the organisation and employees at risk. Failure to comply with any requirement may lead to disciplinary action which may lead to dismissal.

If any employees, customers, third party organisations or stakeholders or other have any concerns of questions regarding the Premier Electrics' stance on the protection of personal data or this policy, please do not hesitate to contact HR.

Eamon M'Ketto

11-6-24