

Data Protection Policy

1. Introduction

Purpose and Scope

This Data Protection Policy outlines Elect's approach to handling personal data in compliance with the General Data Protection Regulation (GDPR) and the UK Data Protection Act. It sets out the key principles and procedures for collecting, processing, and securing personal data to protect the privacy rights of individuals. This policy applies to all employees, contractors, and any third parties processing data on behalf of Elect.

Legal Framework

The policy is designed to ensure compliance with GDPR and the UK Data Protection Act, which govern how personal data must be handled in the UK and EU.

2. Data Protection Principles

Elect follows these key data protection principles to ensure personal data is processed appropriately:

Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, fairly, and transparently. Elect will always inform individuals about how their data is used and ensure processing complies with legal requirements.

Data Minimisation

Only the personal data necessary for specific purposes will be collected and processed. Elect ensures that data processing is limited to what is relevant for its intended use.

Accuracy and Security

Elect takes steps to ensure the accuracy of the data it holds. Personal data is regularly reviewed and updated as necessary. Appropriate security measures are in place to protect personal data from unauthorised access, loss, or damage.

3. Roles and Responsibilities

Data Controller

Elect acts as a Data Controller and is responsible for determining the purposes and means of processing personal data.

Data Processors

Third-party service providers or contractors who process data on behalf of Elect are considered Data Processors. Elect ensures that Data Processors comply with data protection laws through formal agreements.

Employee Responsibilities

All employees must adhere to this Data Protection Policy and follow procedures when handling personal data. Employees are responsible for ensuring that personal data is processed securely and in accordance with company policies.

4. Data Subject Rights

Data subjects (individuals whose data is processed) have the following rights under GDPR:

Access, Rectification, and Erasure

- **Access:** Individuals have the right to request access to their personal data.
- **Rectification:** Individuals can request corrections to inaccurate or incomplete personal data.
- **Erasure:** In certain circumstances, individuals can request the deletion of their personal data (Right to be Forgotten).

Right to Object and Data Portability

- **Right to Object:** Individuals can object to certain types of data processing, including direct marketing.
 - **Data Portability:** Individuals can request that their data be transferred to another service provider in a commonly used, machine-readable format.
-

5. Data Security

Physical and Digital Security Measures

Elect uses appropriate physical security (e.g., secure premises, locked cabinets) and digital security (e.g., encryption, firewalls, secure access systems) to protect personal data.

Access Controls and Encryption

Only authorised personnel have access to personal data. Elect uses encryption to protect data both at rest and in transit, reducing the risk of unauthorised access or data breaches.

6. Data Retention and Disposal

Retention Periods

Elect retains personal data only for as long as necessary to fulfil the purposes for which it was collected. Retention periods are based on legal and business requirements, and personal data is regularly reviewed to ensure it is still needed.

Secure Disposal of Data

Once personal data is no longer needed, it is securely deleted or destroyed. This may include shredding physical documents or using secure deletion software for digital files, ensuring that data cannot be recovered.

7. Data Breaches

Identification and Reporting

A data breach occurs when personal data is accidentally or unlawfully lost, destroyed, accessed, or disclosed. Employees must report any suspected breaches immediately to the Data Protection Officer (DPO) or the designated data protection lead.

Corrective Measures

In the event of a data breach, Elect will assess the scope and impact, notify the relevant authorities (including the ICO within 72 hours if required), and take immediate steps to mitigate any further risks or damages.

8. Policy Review and Updates

This policy is reviewed annually to ensure it reflects current legal requirements and best practices. Updates will be made in response to any changes in data protection laws or regulations, and all employees will be informed of any significant changes to the policy.

