

Data Retention Policy.

Table of Contents.

PURPOSE.	2
POLICY STATEMENT.	2
DEFINITIONS.	2
TYPES OF DATA	2
SCOPE.	4
RESPONSIBILITIES.	4
DATA RETENTION	5
DATA STORAGE AND PROTECTION.	5
ACCESS CONTROLS	5
DATA DISPOSAL.	5
EMPLOYEE TRAINING AND AWARENESS.	5
WHO TO CONTACT.	5
DOCUMENT REVISIONS.	6

Purpose.

The purpose of this policy is to outline the guidelines and procedures for the retention and deletion of data within eEnergy. Its purpose is to guarantee compliance with all applicable legal and regulatory mandates, safeguard data privacy and security, and promote efficient data management practices within the organisation.

Policy Statement.

eEnergy will comply with all applicable laws, regulations, and industry standards related to data retention and protection, including but not limited to the General Data Protection Regulation (GDPR) and any other relevant data privacy legislation.

Review and Audit

This data retention policy shall be reviewed and audited periodically, either every 2 years or where there are changes to legislation. Any updates or changes will be documented and communicated to all relevant personnel.

Definitions.

Types of Data

This policy covers all data collected, generated, or processed by eEnergy including, but not limited to:

- **Customer Information:** This involves data pertaining to our clients, such as contact details, account information, transaction history, preferences, and feedback. This information is crucial for delivering services, managing relationships, and enhancing customer experiences.
- **Financial Records:** Financial data includes invoicing, billing, and payment information, as well as credit reports and financial statements. These records are vital for accounting, compliance, auditing, and other financial management processes within eEnergy.
- **Employee Data:** This category covers information related to eEnergy's staff, ranging from personal and contact details to employment history, payroll information, performance evaluations, and benefits enrolment. Employee data supports human resources in effectively managing recruitment, compensation, development, and legal compliance.

- **Intellectual Property:** Intellectual property data comprises proprietary knowledge, trade secrets, patents, copyrights, trademarks, and any documentation related to research, development, and innovation within eEnergy. This data is essential for protecting the company's intangible assets and competitive positioning in the market.
- **Operational Data:** This broad category encompasses information generated or used in the daily functions and activities of eEnergy. It includes, but is not limited to, production schedules, project management data, inventory levels, supply chain information, and quality assurance records. Operational data is indispensable for planning, monitoring, and improving the efficiency and effectiveness of eEnergy's processes and services.
- **Vendor/Supplier Information:** Details about companies or individuals providing products or services to eEnergy, which might include contact information, bank details, tax identification numbers, and service agreements.
- **Marketing Data:** Information collected about potential clients or customers through marketing campaigns, events, or website visits, which may include preferences, demographics, and interactions with marketing materials.
- **Contract Data:** Details contained in contracts or agreements eEnergy has with customers, vendors, partners, or employees.
- **Communication Records:** Logs or records of communications, including emails, chat messages, and voicemails, conducted over eEnergy's network or on company-provided devices.
- **User Access and Authentication Logs:** Records detailing who has accessed specific pieces of data or systems and when, often used for security and compliance purposes.
- **Network and Information Security Data:** Data related to the security and integrity of the company's network and information systems, including IP addresses, device identifiers, and security incident logs.
- **Cookies and Web Analytics Data:** Information collected through the company's website or applications, including usage statistics, browsing history, and user preferences, often through cookies or similar tracking technologies.
- **Legal and Compliance Documentation:** Records necessary for compliance with applicable legal, regulatory, and internal policy requirements.
- **Feedback and Survey Responses:** Information provided voluntarily by individuals through feedback forms, surveys, or reviews related to eEnergy's products, services, or performance.
- **Human Resources Data:** Additional employee-related data not covered under "employee data", like performance reviews, disciplinary records, and training documentation.

Scope.

The provisions of this policy extend to all employees, contractors, and third-party representatives who are entrusted with handling and managing data under eEnergy's purview. This policy is inclusive of all categories of data—whether collected, generated, or processed—by eEnergy.

Responsibilities.

All individuals who are tasked with utilising personal data within the organisation must adhere strictly to the established 'data protection principles'. These fundamental rules stipulate that all personal data must be:

- **Used Fairly, Lawfully, and Transparently:** Data handlers are obligated to ensure that every piece of information is processed justly, in compliance with legal standards, and with a level of transparency that is expected from a responsible entity.
- **Used for Specified, Explicit Purposes:** Information should only be used for reasons that are clearly defined and explained at the time of collection. No data should be used in a manner that is unexpected or not communicated to the data subjects.
- **Used Adequately and Limited to Necessity:** The use of data should be reasonable and proportional to the purposes for which they were collected. Data handlers should not collect or use more data than is absolutely required to fulfil the stated objectives.
- **Accurate and Updated:** Ensuring the accuracy of data is crucial. Data handlers must take reasonable steps to update, correct, or dispose of data that is outdated, incorrect, or incomplete.
- **Kept for No Longer Than Necessary:** Personal data should be retained only for the period required to achieve the purposes for which it was collected. Upon reaching the end of this period, data should be securely deleted or anonymised.
- **Handled Securely:** Adequate measures must be instituted to safeguard data from unauthorised access, disclosure, alteration, and destruction. This includes protection against unlawful processing and against accidental loss, destruction, or damage.

It is incumbent upon all individuals within the scope of this policy to observe these principles diligently and conscientiously to uphold the integrity and confidentiality of the personal data entrusted to eEnergy's care.

Data retention

Data shall be retained for a specified period based on legal requirements, business needs, and industry standards. Any personal data that is collected or processed is to be kept for as long as this data is required to achieve the purpose for which the information was collected only.

Data storage and protection.

All data must be stored in a secure and controlled environment to prevent unauthorised access, loss, or breach. eEnergy will implement appropriate security measures, such as encryption, access controls, and regular data backups, to ensure data protection.

Access controls

Access to data shall be granted on a need-to-know basis. Authorised individuals shall have access only to the data required to perform their job functions. Access controls, user roles, and permissions shall be implemented and regularly reviewed to mitigate the risk of unauthorised access or disclosure.

Data disposal.

Data shall be disposed of in a secure manner once the retention period expires or when it is no longer needed. Disposal methods may include secure deletion, physical destruction, or anonymisation techniques.

Employee training and awareness.

All employees and relevant personnel shall receive training on this data retention policy, including the procedures for data retention and disposal. eEnergy will promote a culture of data protection and privacy awareness among its workforce.

Who to Contact.

If any eEnergy staff member has questions or concerns regarding data retention and deletion practices within the company, they are advised to promptly communicate with their line manager to voice these issues. It is imperative for line managers to document every concern reported and forward them without delay to the Data

Protection Officer (Abi Wall), who will, if necessary, engage external organisations in a timely fashion.

In cases where an employee is uneasy about sharing concerns with their line manager, alternative routes are available. Employees can either reach out to a member of the senior management team directly or use the confidential Protect Whistleblowing Advice Line at 020 3117 2520 to report their concerns anonymously.

Document Revisions.

Policy Version	Last reviewed date/by:		Next review date:
01	September 2023	Mark Sherrard	
02	March 2025	Abi Wall (CPO)	March 2027