

**Data Protection and Privacy Policy Summary**

**EPPH Ltd is registered under the data protection act with the information commissioner’s office (ICO) under registration reference: A8297567**

**Scope**

EPPH Ltd retains certain information about its employees, customers, suppliers and other users to allow it to monitor performance, achievements, health and safety and to comply with manufacturer warranties. It applies to all data that the company relating to identifiable individuals, even if that information falls outside the Data Protection Act 1998. To be compliant with GDPR, information is collected lawfully and used fairly, stored safely and not disclosed to any other person unlawfully, to do this, the company complies with the Data Protection Principles, which are set out in the Data Protection Act 1998.

**Principles**

EPPH Ltd, as far as, reasonably practicable complies with the Data Protection Principles contained in the Data Protection Act to ensure all data is:

* Fairly and lawfully processed
* Processed for a lawful purpose
* Adequate, relevant and not excessive
* Accurate and up to date
* Held for any no longer than is absolutely necessary
* Processed in accordance with the rights of the data subject
* Protected in the appropriate way
* Not transferred to any other countries without adequate protection and consent

**Sensitive Personal Data**

EPPH Ltd ensures there is stronger legal protection for more sensitive information such as:

* Ethnic background
* Political opinions
* Religious beliefs
* Health
* Sexual health
* Gender
* Criminal records

**Responsibilities**

All staff who work for or with EPPH have responsibility for ensuring data is collected, stored and handled in a safe secure and appropriate manner.

**Data Protection Officer**

EPPH Ltd has appointed the Finance Director as the Data Protection Officer dpo@epph.co.uk who will

endeavor to ensure all personal data is processed in compliance with the GDPR and the Data Protection Act 1998.

**Why we need to store your Personal Data**

In order to meet our legal requirements relating to the Sale of Goods Act and Government Institutions such as HMRC and to allow us to provide the service, it is necessary to store basic customer personal information. This information may also be required in order for EPPH Ltd to provide extended warranties on these products and services or if a warranty or repair is to be registered by us with a supplier.

**Data Storage**

Data stored electronically must be protected from unauthorized access, accidental deletion and malicious hacking attempts. We are committed to protecting all Personal Data we collect and use. To that end, we take all reasonable precautions to prevent the loss, misuse or alteration of your

Personal Data held within our data repositories. We use SSL encryption technology wherever payments are made. Our data repositories are only one element in the internet communication chain. With this is mind, please ensure you access our Websites from a trusted browser/computer (we do not advise using shared browsers/computers for order or payment processing). You should ensure your device has sufficient anti-virus or malware protection. You are responsible for keeping your password confidential. We will not ask you for your password and please ensure any password you use is unique to our websites only. Questions about the storage of data can be directed to the Data Governance team.

**Data Accuracy**

EPPH Ltd takes all reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort staff must put in to ensure its accuracy.

**Right of access**

Data subjects have the right of access to information held by EPPH Ltd, if an individual contacts the company requesting this information, this is called “Subject Access Request”. Subject access request from individuals should be made by email, addressed to the Data Governance team via dpo@epph.co.uk and are each charged at £10+vat (the fee must be paid prior to any subject Access Request being carried out.)

**The disclosure of data for other reasons**

In certain circumstances, the Data Protection Act allows personal data to be disclosed to government and law enforcement agencies without the consent of the data subject.

**Providing information**

EPPH Ltd aims to ensure that individuals are aware that their data is being processed. EPPH Ltd will not give, sell, share or trade any Personal Data to any party outside of EPPH Ltd except as outlined in this Policy or with appropriate consent. We may disclose or share Personal Data to a third party in the following limited circumstances:

* to comply with the terms of trading, policies or other contractual requirements of EPPH Ltd
* where we believe that the disclosure is necessary to establish the threat of and prevent or respond to fraud, defend our Websites or infrastructure against possible attacks or protect the property and safety of EPPH Ltd, our Customers, Suppliers or the public
* to the extent that we are required to do so by law or in connection with any legal proceedings or prospective legal proceedings
* in connection with any potential sale, transfer, merger, consolidation or other transaction involving all or part of EPPH Ltd or its holding companies
* where required, provide our vendor partners or suppliers (or their authorised data partners) with information which may contain Personal Data confirming the recipient and delivery address for statistical sell out analysis or for the registering of extended or enhanced warranties (where applicable)
* to companies that provide services that help us with our business activities including but not limited to processing customer payments, logistics and repairs
* to companies that work with us to provide a product or service necessary to meet a customer’s enquiry or requirement

**Website Data**

By visiting any of our Websites, we may collect anonymous information (via cookies) about your computer and your visits to our Websites such as your IP address, geographical location, browser type, referral source, length of visit and number of page views. We may use this information in the administration of our Websites or to improve the website's usability. This information may be recorded by a third party on our behalf.

If you register or create an account directly on any of our Websites or via a third party procurement system (usually in preparation to purchase from us), we may collect and store some basic personal information mainly (but not limited to) your name, address, email, company or institution and telephone number to allow us to fulfil our obligations to you when processing an order.

**Marketing to you**

We may send you marketing communications relating to our business which we think may be of interest to you (providing you have opted in to receive such information or not opted out or unsubscribed if you have previously had a contractual relationship with us by purchasing a product or service). If you are a business (non-consumer) contact working for a business or institution who we have had a previous contractual history with, or again as a non-consumer contact you have been referred to us by one of our suppliers or vendors following your enquiry to them, we may add your contact information to our business CRM system. We will, however, ask you to opt into receiving marketing communication before sending any marketing information to you.

**CCTV**

EPPH operates a CCTV network for the purposes of crime prevention, detection and safeguarding personnel and property.

This policy summarizes the main EPPH Ltd Data Protection policy written in compliance to GDPR and the Data Protection Act 1998 and is reviewed on a regular basis by Senior Management. You should revisit this page occasionally to ensure you are happy with any changes.

**EPPH GDPR Compliance**

**Programme to comply with GDPR**

1. **Assessment and Awareness**: The first step is to assess the current data handling practices within the company and raise awareness among employees about the importance of GDPR compliance.
2. **Data Audit**: EPPH Conduct a thorough audit of all data collected, stored, and processed by the company. This includes identifying what personal data is being collected, where it's stored, how it's processed, and who has access to it.
3. **Data Mapping and Classification**: EPPH Map out the flow of personal data throughout the organization and classify it based on sensitivity and risk. This helps in understanding the level of protection required for different types of data.
4. **Privacy Policies and Notices**: EPPH review and update privacy policies and notices to ensure they are transparent, easily understandable, and compliant with GDPR requirements. This includes informing individuals about the purpose of data collection, their rights regarding their personal data, and how it will be processed.
5. **Consent Management**: Implement mechanisms for obtaining and managing consent for data processing activities. Ensure that consent is freely given, specific, informed, and unambiguous.
6. **Data Subject Rights**: Establish procedures for facilitating data subject rights such as access, rectification, erasure, and data portability. Ensure that individuals can exercise these rights easily and promptly.
7. **Data Security Measures**: EPPH have Implemented appropriate technical and organizational measures to ensure the security of personal data. Inclusive of encryption, pseudonymization, access controls, and regular security assessments.
8. **Data Breach Response Plan**: EPPH have Developed and document a data breach response plan outlining the steps to be taken in the event of a data breach. This includes notifying the appropriate supervisory authorities and affected individuals within the required timeframes.
9. **Vendor Management**: EPPH evaluate the data processing activities of third-party vendors and ensure that they are GDPR compliant. This may involve updating contracts to include GDPR requirements and conducting regular assessments of vendor compliance.
10. **Training and Education**: Provide regular training and education to employees on GDPR requirements, data protection best practices, and their responsibilities in ensuring compliance.
11. **Ongoing Monitoring and Review**: Continuously monitor and review data processing activities to ensure ongoing compliance with GDPR requirements. This includes conducting regular audits, assessments, and reviews of policies and procedures.
12. **Documentation and Record-Keeping**: Maintain detailed records of data processing activities, assessments, audits, and compliance efforts to demonstrate accountability and compliance with GDPR requirements.

 By following these steps and continuously monitoring and adapting to changes in GDPR regulations, companies can work towards achieving and maintaining GDPR compliance.

Handling sensitive materials and data defined and assigned throughout the organization to ensure compliance with data protection regulations such as GDPR.

**Responsibilities for handling sensitive materials**

**Senior Management/Board of Directors**:

* + Set the tone for the organization's commitment to data protection and compliance.
	+ Approve data protection policies and allocate resources for their implementation.
	+ Appoint a Data Protection Officer (DPO)
	+ Review reports on data protection compliance and breaches.

**Data Protection Officer (DPO)**:

* + Serve as the primary point of contact for data protection authorities and individuals regarding data protection matters.
	+ Monitor compliance with data protection regulations, including GDPR.
	+ Provide advice and guidance to the organization and its employees on data protection obligations.
	+ Conduct or oversee data protection impact assessments (DPIAs) when necessary.
	+ Act as a liaison between the organization, data subjects, and regulatory authorities.

**Data Controllers**:

* + processing personal data.
	+ Ensure that data processing activities are carried out in compliance with data protection regulations and organizational policies.
	+ Obtain appropriate consent from data subjects where required.
	+ Implement measures to protect the rights of data subjects, including access, rectification, erasure, and data portability.
	+ Maintain records of processing activities as required by GDPR.

**Data Processors**:

* + Process personal data on behalf of data controllers in accordance with their instructions.
	+ Implement appropriate technical and organizational measures to ensure the security of personal data.
	+ Comply with contractual obligations regarding data protection and security.
	+ Notify the data controller of any data breaches without undue delay.
	+ Assist the data controller in fulfilling data subject rights requests.

**Employees**:

* + Handle sensitive materials and data in accordance with organizational policies and procedures.
	+ Attend data protection training sessions to understand their responsibilities and obligations.
	+ Report any potential data breaches or security incidents to the appropriate authorities within the organization.
	+ Exercise caution and discretion when accessing, processing, or sharing sensitive data.
	+ Follow protocols for data retention and disposal to ensure compliance with data protection regulations.

**IT Department**:

* + Maintain technical measures to ensure the security and integrity of sensitive data.
	+ Monitor network traffic and access logs for suspicious activity.
	+ Regularly update software and systems to address security vulnerabilities.
	+ Conduct regular security assessments and penetration testing to identify and mitigate risks.
	+ Provide support and guidance to employees on secure handling of data and use of IT systems.

**Legal and Compliance Department**:

* + Monitor changes in data protection laws and regulations and update organizational policies accordingly.
	+ Conduct privacy impact assessments (PIAs) or DPIAs for new projects or initiatives involving the processing of personal data.
	+ Provide legal advice and guidance on data protection matters.
	+ Represent the organization in communications with data protection authorities or in legal proceedings related to data protection issues.

**Arrangements in place regarding IT Data Security**

**Access Controls**:

* + EPPH Enforce strong authentication mechanisms such as multi-factor authentication (MFA) for accessing sensitive systems and data.
	+ Regularly review and update user access permissions to prevent unauthorized access.

**Network Security**:

* + EPPH Utilize firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation to protect against unauthorized access and malicious activities.
	+ Encrypt network traffic, especially for sensitive data transmissions, using protocols like SSL/TLS.
	+ Conduct regular vulnerability assessments and penetration testing to identify and mitigate security weaknesses in the network infrastructure.

**Data Encryption**:

* + EPPH encrypt sensitive data at rest and in transit using strong encryption algorithms to prevent unauthorized access in case of data breaches or theft.
	+ Implement encryption for data stored on servers, databases, endpoints, and removable storage devices.
	+ All laptops/ Hardware are password protected
	+ Virus scans are perfomed on a regular basis
	+ Adaptive firewall’s are present on all server / Hardware

**Data Loss Prevention (DLP)**:

* + EPPH have Implemented DLP solutions to monitor and prevent unauthorized transmission of sensitive data outside the organization's network.
	+ Define policies to classify and tag sensitive data, and enforce rules to prevent data leakage via email, web uploads, or other channels.

**Security Patch Management**:

* + Regularly monitor vendor advisories, security forums, and threat intelligence sources for information on emerging security threats and patches.

**Data Backup and Recovery**:

* + automated and regular backups of critical data to ensure its availability in case of accidental deletion, hardware failure, or ransomware attacks.
	+ Test backup and recovery procedures periodically to verify data integrity and effectiveness of recovery processes.

**Security Awareness Training**:

* + Regular training and awareness programs to educate employees about security best practices, phishing attacks, and social engineering techniques.
	+ Conduct simulated phishing exercises to assess employee readiness and reinforce training.

**Compliance and Auditing**:

* compliance with relevant data protection regulations, industry standards, and contractual obligations related to data security.
* internal audits to assess adherence to security policies, standards, and regulatory requirements.

**Data Protection training for staff**

**Introduction to Data Protection Regulations**:

* Overview of relevant data protection regulations (e.g., GDPR) and their key principles.
* Explanation of the importance of data protection for individuals, organizations, and society.
* Introduction to the roles and responsibilities of employees in safeguarding personal data.

**Understanding Personal Data**:

* Definition of personal data and its different categories (e.g., identifiable, sensitive).
* Examples of personal data commonly handled by employees in their roles.
* Explanation of the concept of data minimization and the need to collect only necessary data.

**Principles of Data Processing**:

* Explanation of the lawful bases for processing personal data under GDPR.
* Overview of the principles of fairness, transparency, and accountability in data processing.
* Discussion of data subject rights (e.g., right to access, rectification, erasure) and how employees should handle requests from data subjects.

**Data Security Best Practices**:

* Importance of data security measures in protecting personal data from unauthorized access, disclosure, and alteration.
* Explanation of technical and organizational security measures (e.g., encryption, access controls, password management) and their implementation.
* Guidance on securely handling, storing, and transmitting personal data both physically and electronically.

**Handling Data Breaches**:

* Definition of a data breach and examples of common causes.
* Procedures for reporting and escalating suspected or confirmed data breaches within the organization.
* Roles and responsibilities of employees in responding to data breaches and mitigating their impact.

**Privacy by Design and Default**:

* Explanation of the principles of privacy by design and default and their relevance to product and system development.
* Guidance on integrating privacy considerations into business processes, product design, and system architecture from the outset.

**Data Protection Impact Assessments (DPIAs)**:

* Overview of DPIAs and their purpose in identifying and mitigating risks to individuals' privacy.
* Explanation of when and how DPIAs are conducted within the organization.

**Social Engineering and Phishing Awareness**:

* Recognition of common social engineering tactics used by attackers to gain unauthorized access to personal data.
* Guidance on identifying phishing emails, malicious links, and suspicious requests for personal information.
* Best practices for responding to and reporting phishing attempts.
* **Practical Scenarios and Case Studies**:
* Interactive exercises and case studies to reinforce learning and help employees apply data protection principles in real-world scenarios.
* Discussion of past data protection incidents and their implications for the organization.
* **Regular Updates and Refresher Training**:
* Emphasis on the need for ongoing training and awareness to stay abreast of changes in data protection regulations, emerging threats, and best practices.
* Schedule regular refresher sessions to reinforce key concepts and address any new developments.
* **Assessment and Certification**:
* Assessment mechanisms (e.g., quizzes, exams) to evaluate employees' understanding of data protection concepts and identify areas for improvement.
* Provision of certificates or badges upon successful completion of training to recognize and incentivize participation.
* **Documentation and Records Management**:
* Importance of maintaining records of training attendance, completion, and outcomes for compliance and auditing purposes.
* Procedures for accessing and updating training materials and resources as needed.

**All server and external hosting done by Connection Technologies LTD. In-house permissions and safeguarding are overseen via the Operations Manager.**

**DATA Security**

**All sever & Hardware access are governed via Password / Encryption protected access.**



Signed:

Managing Director

EPPH Ltd

Date: 04/01/2024