ECM Privacy Standard

Version 1.0
Effective Date 25th May 2018

Introduction

ECM needs to collect, handle and store certain information about living individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This privacy standard describes how this personal data must be collected, handled and stored in order to meet the company's data protection standards and to comply with the law.

Purpose

This privacy standard ensures ECM:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The General Data Protection Regulation (GDPR) introduced in May 2018 describes how organisations, including ECM, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

The GDPR has key principles of compliance.

ECM adheres to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

ECM is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

Scope of this Privacy Standard

This standard applies to:

- The head office of ECM
- All branches of ECM
- All staff of ECM
- All contractors, suppliers and other people working on behalf of ECM
- It applies to all data that the company collects, processes and stores relating to identifiable individuals.

Data Protection Risks

This privacy standard helps to protect ECM from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with ECM has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this standard and data protection principles.

However, these people have key areas of responsibility:

- The **Board of Directors** are ultimately responsible for ensuring that ECM meets its legal obligations.

- The **Finance Director**, is responsible for:
  o Keeping the board updated about data protection responsibilities, risks and issues.
  o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  o Arranging data protection training and advice for the people covered by this standard.
  o Handling data protection questions from staff and anyone else covered by this standard.
  o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **IT Manager**, is responsible for:
  o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  o Performing regular checks and scans to ensure security hardware and software is functioning properly.
  o Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The **Personnel Manager**, is responsible for:
  o Dealing with requests from individuals to see the data ECM holds about them (also called "subject access requests")

General Staff Guidelines

- The only people able to access data covered by this standard should be those **who need it for their work.**
- Data should **not be shared informally**. When access to confidential information is required, employees can request it from their line managers.

  Generally ECM is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

  We may only share the Personal Data we hold with another employee, agent or representative of ECM if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

  We may only share the Personal Data ECM holds with third parties, such as ECM's service providers if:

  (a) they have a need to know the information for the purposes of providing the contracted services;

  (b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

  (c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and

(d) a fully executed written contract which contains appropriate GDPR-related clauses has been entered into.

- **ECM will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared between employees.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found by your Departmental Manager to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the **Finance Director** if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services.**
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

The GDPR requires ECM to keep full and accurate records of all our data processing activities.

We must keep and maintain accurate corporate records reflecting our processing of personal data.

Data Use

It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the **screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees should **not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data Accuracy

The law requires ECM to take 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 ECM should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- ECM will make it **easy for data subjects to update the information** ECM holds about them.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

All individuals who are the subject of personal data held by ECM are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request and will be dealt with by the Personnel Manager under the rights of access under GDPR.

ECM will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for Other Reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ECM will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing Information

ECM aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. A version of this statement is also available on the company's website.

ECM (Vehicle Delivery Service) Ltd
The Airport
Carlisle,
United Kingdom, CA6 4NW

END