GDPR – Data Protection Policy

Context and Overview

Introduction

CMB Engineering needs to gather and use certain information about individuals.

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

This policy describes how this personal data must be collected, managed, and stored to meet the company's data protection standards – in line with GDPR guidelines.

Why this policy exists.

This data protection policy ensures CMB Engineering:

- Complies with data protection law and follows 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 Data Protection Act 2018 describes how organisations – including CMB Engineering – must collect, handle and store personal information.

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

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant, and not excessive.
4. Be accurate and kept up to date.

5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensured an adequate level of protection.

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- The head office of CMB Engineering
- All CMB employees and workers
- Volunteers, interns, and work experience students
- All contractors, suppliers and other people working on behalf of CMB Engineering

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses.
- Telephone numbers.
- Other contact details
- Sensitive or personal data, such as data revealing racial or ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs.
- Health-related data or details of medical conditions
- Any other information relating to individuals.

Data Protection Risks

This policy helps to protect CMB Engineering from some very real data security risks, including:

- Breaches of confidentiality – For instance, information being given out inappropriately and without consent
- Failing to offer choice - For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage – For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with CMB Engineering has some responsibility for ensuring data is collected, stored, and managed appropriately. Each team that manages personal data must ensure that it is managed and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is responsible for ensuring that CMB Engineering meets its legal obligations.
- The data protection officer is responsible for:
    - Keeping the board updated about data protection responsibilities, risks, and issues.
    - Reviewing all data protection procedures and related policies, in line with and agreed schedule.
    - Arranging data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see date that CMB Engineering holds about them (a Subject Access Request)
    - Checking and approving any contracts or agreements with third parties that may manage the company's sensitive data.

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

General Staff Guidelines

- The only people able to access data covered by this policy 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 be completing a **Request for Personal Details form.**
- **CMB Engineering 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.
- **Strong passwords must be used** and should **never** be shared.
- 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 to be out of date or if no longer required, it should be deleted and disposed of

- Employees **should request help** from their line manager or data protection officer if they are unsure about any aspect of data protection.

Data Storage

Thes rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Data Controller.

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 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 left 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 removeable media** (like DVD or CD), it should be kept locked away securely when not be used.
- Data should only be stored on **designated drives and servers** if it cannot be uploaded to an **approved cloud computing service.**
- 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 evaluated regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data Use

Personal data is of no value to CMB Engineering unless the business can make use of it. However, 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**. It should never be sent by mail, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT Manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside the European Economic Area (EEA)**
- 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 CMB Engineering to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that personal data is accurate, the greater the effort CMB Engineering 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 kept 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.
- CMB Engineering will make it easy for **data subjects to update the information** CMB Engineering holds about them. For example, information held via the company website.

Subject Access Rights

All individuals who are the subject of personal data held by CMB Engineering 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.

Subject access requests from individuals should be made by e-mail, addressed to the data controller.

The data controller will aim to provide the relevant data within 14 days but no longer than a month.

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

The company may refuse or charge for requests that are unfounded or excessive.

If a subject access request is refused, the individual must be told the reasons for the refusal, and they must be made aware that they have the right to complain to the supervisory authority and to a judicial remedy. This must be done without undue delay and at the latest, within one month.

Signed:  **Date: 01st January 2025**

John Green
Operations Director