METCOR

Data Protection Policy

Version 1.0 — May 21st, 2026

Open in Waybook

Waybook

Table of Contents

1 Introduction & Scope 3

2 Data Protection Principles 4

3 Lawful Bases for Processing 5

4 Individual Rights 6

5 Data Security & Breach Management 7

6 Data Retention & Third Parties 8

1 Introduction & Scope

Introduction

Metcor is committed to protecting the privacy and security of personal data held in relation to its employees, clients, contractors, and other individuals with whom it conducts business. This policy sets out the framework under which Metcor collects, processes, stores, and manages personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

All employees, contractors, consultants, and third parties acting on behalf of Metcor are required to adhere to this policy. Failure to comply may result in disciplinary action and, where applicable, regulatory or legal consequences.

Scope

This policy applies to:

- All personal data processed by Metcor, whether held electronically or in physical format
- All employees, temporary staff, contractors, and third-party service providers
- All systems, platforms, and tools used to collect or process personal data on behalf of Metcor

What is Personal Data?

Personal data is any information that can identify a living individual, either directly or indirectly. This includes, but is not limited to, names, addresses, email addresses, telephone numbers, identification numbers, and location data. **Special category data** — such as health information, racial or ethnic origin, and biometric data — is afforded additional protections under UK GDPR and must be handled with the utmost care.

Data Controller

Metcor acts as the **data controller** for personal data processed in the course of its business operations. As data controller, Metcor is responsible for determining the purposes and means of processing personal data and for ensuring that all processing activities are lawful, fair, and transparent.

Any questions regarding this policy or Metcor's data protection obligations should be directed to the designated Data Protection Officer (DPO) or appropriate senior manager responsible for data protection compliance.

2 Data Protection Principles

Data Protection Principles

Metcor's approach to data protection is founded on the six core principles set out in Article 5 of the UK GDPR. All personal data processed by or on behalf of Metcor must be handled in accordance with these principles at all times.

The Six Principles

1. Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, fairly, and in a transparent manner. Individuals must be informed about how their data is being used, and processing must be based on a valid lawful basis such as consent, contractual necessity, legal obligation, or legitimate interest.

2. Purpose Limitation

Personal data must be collected for specified, explicit, and legitimate purposes. It must not be further processed in a manner incompatible with those original purposes. Metcor must document the purpose of all data collection activities.

3. Data Minimisation

Only personal data that is adequate, relevant, and limited to what is necessary for the intended purpose should be collected and processed. Employees must not collect data beyond what is required to fulfil a defined business need.

4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that inaccurate data is corrected or deleted without delay. Individuals have the right to request corrections to their personal data.

5. Storage Limitation

Personal data must not be retained for longer than is necessary for the purposes for which it was collected. Metcor maintains a data retention schedule that specifies appropriate retention periods for different categories of data.

6. Integrity and Confidentiality

Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage. This requires the implementation of appropriate technical and organisational security measures.

> All staff handling personal data are personally responsible for adhering to these principles. Ignorance of the policy does not constitute a defence in the event of a breach.

3 Lawful Bases for Processing

Lawful Bases for Processing

Metcor must identify and document a valid lawful basis before processing any personal data. Processing without a lawful basis constitutes a breach of UK GDPR. The lawful bases available under UK GDPR are outlined below, along with guidance on how they apply within Metcor's operations.

Applicable Lawful Bases

Contractual Necessity

Where processing is necessary to fulfil a contract with an individual, or to take steps at their request prior to entering into a contract. This is the primary basis for processing employee and client personal data.

Legal Obligation

Where processing is required to comply with a legal obligation placed on Metcor. This includes obligations under employment law, health and safety legislation, and environmental regulations applicable to Metcor's operations.

Legitimate Interests

Where processing is necessary for Metcor's legitimate business interests, provided those interests are not overridden by the rights and freedoms of the individual. A Legitimate Interests Assessment (LIA) must be completed and documented before relying on this basis.

Consent

Where an individual has freely given, specific, informed, and unambiguous consent to the processing of their personal data. Consent must be documented and can be withdrawn at any time. Consent is not the preferred basis for employment-related processing due to the imbalance of power between employer and employee.

Vital Interests and Public Task

These bases apply in limited circumstances and are less commonly relied upon within Metcor's day-to-day operations.

Special Category Data

Processing special category data requires both a lawful basis under Article 6 and an additional condition under Article 9 of UK GDPR. Common conditions used by Metcor include:

- Employment, social security, and social protection law obligations
- Occupational health and safety purposes
- Explicit consent of the data subject All instances of special category data processing must be reviewed and approved by the DPO or designated senior manager prior to commencement.

4 Individual Rights

Individual Rights

UK GDPR grants individuals a set of rights in relation to their personal data. Metcor is obligated to respect and facilitate these rights in a timely and transparent manner. All requests must be handled without undue delay and, in most cases, within **one calendar month** of receipt.

Rights Available to Individuals

Right of Access

Individuals may request a copy of the personal data Metcor holds about them, along with information about how it is being used. This is known as a Subject Access Request (SAR).

Right to Rectification

Individuals may request that inaccurate or incomplete personal data be corrected. Metcor must act on such requests promptly.

Right to Erasure

Also known as the "right to be forgotten", individuals may request the deletion of their personal data where it is no longer necessary, where consent has been withdrawn, or where it has been unlawfully processed.

Right to Restrict Processing

Individuals may request that Metcor limits how their data is used while a dispute or review is ongoing.

Right to Data Portability

Where processing is based on consent or contract and is carried out by automated means, individuals may request their data in a structured, commonly used, and machine-readable format.

Right to Object

Individuals may object to processing based on legitimate interests or for direct marketing purposes. Metcor must cease processing unless compelling legitimate grounds can be demonstrated.

Handling Requests

All requests relating to individual rights should be directed to the DPO or designated data protection contact. Staff must not attempt to handle such requests independently. Key obligations include:

- Verifying the identity of the requestor before disclosing any information
- Logging all requests and their outcomes
- Escalating complex or sensitive requests to senior management or legal counsel where necessary Metcor will not charge a fee for handling rights requests unless they are manifestly unfounded or excessive.

5 Data Security & Breach Management

Data Security & Breach Management

Metcor takes the security of personal data seriously and has implemented a range of technical and organisational measures to protect data against unauthorised access, loss, destruction, or disclosure. All staff share responsibility for maintaining data security within their area of work.

Security Measures

Metcor employs the following measures to safeguard personal data:

- Access controls and user authentication on all systems holding personal data
- Encryption of sensitive data in transit and at rest where technically feasible
- Regular security patching and software updates across IT infrastructure
- Physical access controls for premises where personal data is stored
- Staff training and awareness on data protection and information security Employees must not share login credentials, access personal data from unsecured networks without appropriate protection, or store personal data on unauthorised devices or platforms.

Data Breach Response

A personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All suspected or confirmed breaches must be reported immediately to the DPO or designated data protection contact.

> Any employee who becomes aware of a potential data breach must report it without delay. Delayed reporting may worsen regulatory consequences and increase risk to affected individuals.

Upon notification, Metcor will:

1. Assess the nature and severity of the breach
2. Take immediate steps to contain and mitigate the impact
3. Determine whether notification to the Information Commissioner's Office (ICO) is required within **72 hours**
4. Notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms
5. Document the breach, its impact, and the remedial actions taken All breaches, regardless of severity, must be recorded in Metcor's internal breach register. This record supports ongoing compliance monitoring and regulatory accountability.

6 Data Retention & Third Parties

Data Retention & Third Parties

Data Retention

Metcor retains personal data only for as long as is necessary for the purposes for which it was collected, or as required by applicable law or regulation. Retaining data beyond its required period unnecessarily increases risk and may constitute a breach of UK GDPR's storage limitation principle.

Metcor maintains a **Data Retention Schedule** which sets out the defined retention periods for all major categories of personal data held by the organisation. This schedule is reviewed annually and updated as necessary to reflect changes in business operations or legal requirements.

When personal data reaches the end of its retention period, it must be securely disposed of in an appropriate manner:

- Electronic data should be permanently deleted or overwritten using approved methods
- Physical records containing personal data must be shredded or disposed of via a secure destruction service
- Disposal must be documented, particularly for special category data

Third-Party Data Processing

Where Metcor engages third parties to process personal data on its behalf — such as IT service providers, payroll processors, or occupational health providers — those parties are classified as **data processors**. Metcor remains responsible for ensuring that data processors provide sufficient guarantees regarding their data protection practices.

Before engaging a data processor, Metcor must:

- Conduct appropriate due diligence on the processor's data protection arrangements
- Ensure a written Data Processing Agreement (DPA) is in place that meets UK GDPR requirements
- Confirm that the processor will only act on Metcor's documented instructions **International transfers** of personal data outside the United Kingdom are only permitted where an appropriate safeguard is in place, such as an adequacy decision, standard contractual clauses, or binding corporate rules. Any proposed international transfer must be reviewed and approved by the DPO prior to data being shared. All third-party arrangements involving personal data must be reviewed periodically to ensure ongoing compliance with this policy and applicable data protection law.