

POL109 - The General Data Protection Regulation (GDPR)



The GBM GDPR Policy outlines the organisation's commitment to data protection, compliance with GDPR - as well as compliance with best-practice standards (ISO 27001 and Cyber Essentials). It defines GBM's roles as a Data Processor and Data Controller, specifying how data is handled securely, responsibly, and lawfully.

Data Processor

Where GBM is acting as a Data Processor, it will not process data unless instructed to do so by the Data Controller. Whilst processing data on behalf of a Data Controller, GBM will ensure that:

- All data is stored securely
- The terms of the processing agreement are upheld (including data retention)
- It supports the Data Controller in responding to requests relating Data Subject Rights (such as Subject Access Requests)

Data Controller

Where GBM is acting as a Data Controller, it will be responsible designating how and why Personal Data is collected and used, as well as establishing the legal basis for collecting and processing the data. GBM may contract one or more Data Processor/s to help carry-out processing activity.

Lawful Basis for Processing Data

In order to operate in its market, GBM rely on processing Personal Data, and as such, must establish grounds for processing the data that it collects.

For example, GBM may need to collect and process Personal Data in order to provide

products and services to businesses, educational establishments, and consumers.

In this instance, GBM may rely on the 'Contract' basis as the lawful basis for processing data, which includes:

- Processing data in order to fulfil it's obligations to a Data Subject (such as processing their order)
- Carrying-out, at the Data Subject's request, preliminary activities that lead to the sale, such as arranging a quotation

Privacy

A full privacy notice is clearly published on our websites (gbm-group.co.uk, wearesync.co.uk, kingsfieldit.com), detailing:

- Who we are, and how we collect data
- Where/how data is stored
- How long data is retained for
- The types of data we collect
- How we use data
- Who data may be disclosed to, and why
- Data Subject Rights

Where Personal Data is Stored

GBM may store your Personal Data in both electronic and paper-based formats, utilising the following security mechanisms to ensure that your Personal Data is secure:

- Our electronic systems (including email, and databases) are hosted within the European Economic Area (EEA)
- In order to process Apple repairs we will share Personal Data with Apple, via their 'Global Service Exchange' online repair database. Further details on Apple's privacy policy and data storage capabilities available here: <https://www.apple.com/legal/privacy/en-ww/>

POL109 - The General Data Protection Regulation (GDPR)



- GBM do not store Sensitive Personal Data relating to its customers, such as Debit or Credit card details (merchant copy card receipts are stored / archived in print format, and are securely stored for HMRC compliance, Fraud Prevention and Dispute Resolution).

Data Protection

GBM maintains a Data Protection Policy (POL108), which details:

- How it protects data
- Individual responsibilities for data protection
- General staff guidelines
- How data is stored and used

For a copy of this policy, please email us at GDPR@gbmdt.co.uk

Cyber Security

GBM maintains a Cyber Security Policy (POL103), which details the technical systems that GBM has in place to ensure the protection and integrity of electronic data (such as encryption). This policy is built around the Cyber Essentials framework.

For a copy of this policy, please email us at GDPR@gbmdt.co.uk

Data Retention and Minimisation

GBM maintains a Data Retention Policy (POL110), which utilises data categorisation to classify how long data is retained for, and what actions are taken following the expiration of the retention period.

For a copy of this policy, please email us at GDPR@gbmdt.co.uk

Staff Awareness and Training

In order to raise awareness of the changes to Data Protection and privacy, and provide training to its staff, GBM has embedded mandatory, company-wide training which focusses on Security Awareness. This forms a key part of our Data Security Training and Competency Policy (POL111). For a copy of this policy, please email us at GDPR@gbmdt.co.uk

Breach Reporting

Inline with the breach reporting guidelines, GBM will ensure that data breaches are reported to the ICO within 72-hours of initial detection or occurrence of the breach. In order to ensure that GBM can comply with this timeline, GBM has a documented breach reporting procedure (PRO034), which has been made available to all staff.

Disaster Recovery

In order to minimise downtime, and protect itself against the loss of data, GBM have a number of systems in place to help it protect itself against redundancy. Should a disaster occur, GBM has a documented disaster recovery process, which has been made available to all staff, to help ensure that any downtime is kept to an absolute minimum.

Impact Assessments (DPIA)

The impact assessment process helps organisations to identify and reduce the privacy and data protection risks of a project. An example use could be the consideration of deploying new system, which stores, categorises, or processes data in a different way. By undertaking a DPIA prior to deployment, the organisation can understand

POL109 - The General Data Protection Regulation (GDPR)



what impact the new system may have on it's data subjects security and privacy.

GBM has a documented DPIA process (PRO107), which is based on the framework provided by the Information Commissioners Office (ICO), that can be utilised to support in making decisions about changes to data processing.

Supplier Vetting

As part of it's due diligence, GBM vet it's suppliers and service providers to ensure their compliance with the GDPR. Inline with this process, GBM maintains a Supplier Vetting Policy, which details how suppliers are vetted, and how risk is analysed within our supply chain.

Data Subject Rights

Data subject rights are described clearly within our Privacy Notice. In order to process requests from data subjects, GBM has assigned a Data Protection Lead, who will be the point of contact for all enquiries or requests relating to subject rights.

Data Protection Queries

If you have any queries about the way we process or protect data, or would like to understand more about this document, or our processes, you can contact our Data Protection Lead directly:

Name: Scott Bordoni

Phone: 0161 605 3838

Email: Scott.bordoni@wearesync.co.uk

Address: FAO COO, Unit 2.3-2.4, Arbata, 11

Northampton Road, Manchester, M40 5BP