General Data Protection Regulation Policy

Megan Mechanical Services Ltd is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all our legal obligations.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business Purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial regulatory, payroll and business development purposes. Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice. • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests. • Ensuring business policies are adhered to (such as policies covering email and internet use). • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking. • Investigating complaints. • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments. • Monitoring staff conduct, disciplinary matters. • Marketing our business. • Improving services.
Personal Data	"*Personal data*" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

	Personal data we gather may include individuals' name, hme address, phone number, email address, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV.
Special Categories of Personal Data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health/condition, criminal offences, or related proceedings, and genetic and biometric information – any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data Controller	"*Data Controller*" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data Processor	"*Processor*" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	"*Processing*" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destructing.
Supervisory Authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the ICO.

Scope

This policy applies to all team members, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies or guidelines from time to time.

Who is responsible for this policy?

As our Data Protection Officer (DPO), Stephanie Davis has overall responsibility for the day-to-day implementation of this policy, you should contact Stephanie for further information about this policy if necessary (01252 874738 / stephanie.davis@megan-mechanical.co.uk).

General Data Protection Regulation Policy

The Principles

Megan Mechanical Services shall comply with the principles of data protection (the principles) as enumerated in the UK General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The principles are:

1. **Lawful, Fair and Transparent**

   Data collection must be fair, for legal purpose and we must be open and transparent as to how the data will be used.

2. **Limited for its Purpose**
   Data can only be collected for a specific purpose.

3. **Data Minimisation**
   Any data collected must be necessary and not excessive for its purpose.

4. **Accurate**
   The data we hold must be accurate and kept up to date.

5. **Retention**
   We cannot store data longer than necessary.

6. **Integrity and Confidentiality**
   The data we hold must be kept safe and secure.

Fair and Lawful Processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This means that we should not process personal data unless the individual whose details we are processing has consented to this happening. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**
   We hold recent, clear, explicit and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract**
   The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal Obligation**
   We have a legal obligation to process the data (excluding a contract).

4. **Vital Interests**
   Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public Function**
   Processing necessary to conduct a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate Interest**
   The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Megan Mechanical Services ensures that individuals whose data is being processed are informed of the lawful basis for processing their data, as well as the intended purpose via our Privacy Policy.

Sensitive Personal Data, this means data about an individual which is more sensitive and therefore requires more protection. The special categories include information about an individual's:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g., to comply with legal obligations to ensure health and safety at work). Any consent will need to clarify what the relevant data is, which is being processed and to whim it will be disclosed.

The condition for processing special categories or personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Responsibilities

Our Responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

General Data Protection Regulation Policy

Your Responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies at all times
- Comply with this policy at all time
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Responsibilities of the Data Protection Officer

- Keeping the Directors/Senior Management updated about data protection responsibilities, risk and issue
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, Directors and stakeholders
- Responding to individuals such as clients and employees who wish to know data is being on them by us
- Checking and approving with third parties that manage the company's data any contracts or agreements regarding data processing
- Managing and overseeing the Company's data protection complaints procedure
- Maintaining a register of data protection complaints and ensuring complaints are investigated and responded to within the required timescales, please refer to the Customer Complaints Policy (P28).
- Reporting complaint trends, significant issues and corrective actions to Senior Management
  For further information on how data protection compaints are managed, please refer to the Privacy Policy (P11).

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third party services, such as cloud services the company is considering using to store or process data.

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe the information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data Security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password managed to create and store their passwords
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure.

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Rights of Individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. **Right to be Informed**
   - Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, which are written in clear and plain language, particularly if aimed at children.
   - Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. **Right of Access**
   - Enabling individuals to access their personal data and supplementary information.
   - Allowing individuals to be aware of and verify the lawfulness of the processing activities.

3. **Right to Rectification**
   - We must rectify or amend the personal data of the individual if requested because it inaccurate or incomplete.
   - This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

4. **Right to Erasure**
   - We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. **Right to Restrict Processing**
   - We must comply with any request to restrict, block or otherwise suppress the processing of personal data
   - We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. **Right to Data Portability**
   - We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
   - We must provide it in a commonly used, machine-readable format and send it directly to another controller if requested.

7. **Right to Object**
   - We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
   - We must respect the right of an individual to object to direct marketing, including profiling.
   - We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. **Rights in Relation to Automated Decision Making and Profiling**
   - We must respect the rights of individuals in relation to automated decision making and profiling.
   - Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Right to Erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and/or processed.
- Where consent is withdrawn.
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed or otherwise breached data protection laws.
- To comply with legal obligation.
- The processing relates to a child.

How we deal with the right to erasure?

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligations to erase the data. If the individual asks, we must inform them of those recipients.

The Right to Object

Individuals have the right to object to their data being used on grounds relating to their situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e., in the Privacy Notice. We must offer a way for individuals to object.

The Right to Restrict Automated Profiling or Decision Making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

Third Parties

Using Third Party Controllers and Processors

As a data controller and/or processor we must have written contracts in place with any third-party data controllers and/or data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and the rights of data subjects will be respected and protected.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR ad we will protect and respect the rights of data subjects.

Contracts

Our contracts must comply with the standards set out by the ICO and, where possible follow the standard contractual clauses which are available. Our contracts with data controllers and data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions.
- Those involved in processing the data are subject to a duty of confidence.
- Appropriate measures will be taken to ensure the security of the processing.
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract.
- The controller will assist the processor in dealing with subject access requests ad allowing data subjects to exercise their rights under GDPR.
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments.
- Delete or return all personal data at the end of the contract.
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR

General Data Protection Regulation Policy

Criminal Offence Data

Criminal Record Checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the DPO prior to carrying out a criminal record check.

Audits, Monitoring and Training

Data Audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored and how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the DPO and normal procedures.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this Policy. Megan Mechanical Services Ltd will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully at all times.

Training

You will receive adequate training on GDPR and provision of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the DPO.

Reporting Breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. Megan Mechanical Services Ltd has an obligation to report any data breaches to the ICO.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failure
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

General Data Protection Regulation Policy

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.
Please refer to our Data Breach Procedure MMP10.

Failure to Comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

This importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Gerald Ley
19 June 2026