GDPR Policy

1. Introduction

The Company needs to collect and use certain types of information about the Customers that we deliver products and services to and the staff which we employ. This personal information must be collected and dealt with appropriately whether it collected on paper, stored on our server, collected by email, or stored on phones, or recorded on other material and there are safeguards to ensure this under the General Data Protection Regulations

2. Data Controller and Data Protection Officer

Borough Engineering Services Ltd & Throgmorton Mechanical & Electrical Services are the joint Data Controllers for determining the means and purposes of processing personal data under the Regulations. Borough Engineering Services Ltd acts as data controller on behalf of Omni-air. The data controller determines what purposes personal information is held and will be used for.

The Date Protection Officer (DPO) oversees questions in relation to this policy. They are responsible for:

- Monitoring compliance with GDPR and other data protection laws.
- Advising on data protection impact assessments.
- Acting as point of contact for supervisory authorities. (e.g. the ICO)
- Serving as point of contact for data subjects regarding their rights and how their data is processed.

The DPO is Amit Sharma (A.Sharma@borough-es.co.uk) for all companies mentioned above.

3. Disclosure

BES/TMES only share personal information pertaining to employees with our Chartered Accountant for the purpose of processing payroll and with our Sub-Contractors for the process of providing products in line with specification and for deliveries. BES/TMES will not share information with any other companies or agencies unless legally bound to do so.

If Information is shared for any reason, the Employee/Customer will be made aware in how and with whom their information will be shared. There are circumstances where the law allows BES/TMES to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State

b) Protecting vital interests of an Employee / Customer or other person

c) The Employee / Customer has already made the information public

d) Conducting any legal proceedings, obtaining legal advice, or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e., race, disability, or religion

f) Providing a confidential service where the Employee's / Customer's consent cannot be obtained or where it is reasonable to proceed without consent: e.g., where we would wish to avoid forcing stressed or ill Employee's / Customer's to provide consent signatures.

BES/TMES regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

BES/TMES intends to ensure that personal information is treated lawfully and correctly.

To this end, BES/TMES will adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulations

Specifically, the Principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

b) Shall be obtained only for one or more of the purposes specified in the Regulations, and shall not be processed in any manner incompatible with that purpose or those purposes,

c) Shall be adequate, relevant, and not excessive in relation to those purpose(s)

d) Shall be accurate and, where necessary, kept up to date,

e) Shall not be kept for longer than is necessary,

f) Shall be processed in accordance with the rights of data subjects under the Act,

g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Employee's / Customers in relation to the processing of personal information.

BES/TMES will, through appropriate management and strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information

- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Regulations. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and Organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

4. Data collection

Data Collected by BES/TMES in the most part is collected under the lawful basis of having a contract in place i.e. an employment contract is in place or an order has been placed to progress with works. Where a contract is not in place the lawful basis will be consent which is received in an appropriate manner as follows: -

- An Employee / Customer clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent.

BES/TMES will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, BES/TMES will ensure that the Employee / Customer:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Employee / Customer decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

e) Has received sufficient information on why their data is needed and how it will be used

5. Data Storage

Information and records relating to Customers will be stored securely and will only be accessible to authorised staff.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is BES/TMES responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

6. Data access and accuracy

All Employee's / Customers have the right to access the information BES/TMES holds about them. BES/TMES will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition**,** BES/TMES will ensure that:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the way it holds, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

7. Retention and Disposal of Information

Retention

Records should be kept for as long as they are needed to meet the operational needs of BES/TMES but no less than 7 years, together with legal and regulatory requirements. We have assessed our records to:

- determine their value as a source of information BES/TMES, its operations, relationships, and environment,
- determine their value as a source of valuable information regarding customers, their conditions, and treatments.
- assess their importance as evidence of business activities and decisions
- establish whether there are any legal or regulatory retention requirements (including: Public Records Act 1958, General Data Protection Regulations, the Freedom of Information Act 2000, and the Limitation Act 1980).

Disposal

We set out retention periods for data within the Record register IMS-SYS-001.

Records on disposal schedules will be as follows:

Destroy after an agreed period – where predetermined as 7 years for all normal records the company holds, or a pre-determined time as defined by clients.

Records can be destroyed in the following ways:

Destruction

- Non-sensitive information – can be disposed of by recycling.

- Confidential information – crosscut shredding and/or confidential recycle service.

- Electronic equipment containing information - will be permanently deleted from the system.

Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

Sharing of information

Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retained in accordance with the guidelines detailed above. Care should be taken that seemingly duplicate records have not been annotated.

Where we share information with other bodies, we will ensure that they have adequate procedures for records to ensure that the information is managed in accordance with the relevant legislation and regulatory guidance.

Document Deletion / Disposal

A record / log of deletions and disposals must be maintained on Form IMS-GDPR-002. This should include: -

- the details of the record
- the type of record
- the retention periods
- the reason for deletion / disposal
- the method of deletion / disposal
- the person responsible for the deletion / disposal

In the event of a data breach

In the event of a data breach by loss of information whether in hard copy or electronic copy or a malware or ransomware virus on a company pc or server that removes data we will:

- Address the physical breach by shutting down systems and processes to ensure the data breach does not continue.
- Fully investigate the breach to determine why and how this happened and put in place measures to prevent the re-occurrence of the breach.
- Determine whether the information is high risk information or low risk information. High Risk information is determined as any information that can cause harm to an individual or business.
- If the breach is High Risk Information, then BES/TMES will notify the ICO and the victim of the data breach (the person or company that the data pertains to) within 72 hours of the data breach.
- If the breach is low risk, then BES/TMES will advise the victim of the data breach in writing within 14 days.

Personal Information on Employees or Customer's

BES/TMES will provide all information pertaining to an employee or customer to the employee or customer that the information pertains to within one month of receipt of the request. This will either be provided in a hard copy format or emailed.

Where employees or customers are no longer employees or customers of BES/TMES we will provide information in the same manner as detailed above within one month

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulations

In case of any queries or questions in relation to this policy please contact Amit Sharma who is the DPO

Managing Director	Signature	Date
Jeff Pollitt		01/09/2025