Data Protection Policy

Policy Statement

The Briggs Group is committed to being transparent about how it collects and uses personal information about individuals, including clients, suppliers, business contacts, employees, job applicants and other people the organisation has a relationship with or may need to contact.

This policy describes how personal data must be collected, handled, and stored to meet the Company's data protection standards and to comply with the UK General Data Protection Regulations.

This data protection policy ensures The Briggs Group:

- Complies with the general data protection regulations and follows good practice
- Protects the rights of staff, clients, partners, and others
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Definitions

"**Personal Data**" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including, collecting, storing, amending, disclosing, or destroying it.

"**Special categories of personal data**" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"**Criminal records data**" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Law

The UK General Protection Regulation (UK GDPR) is underpinned by the principles of The Data Protection Act 1998 which still applies, and these are:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.

- The organisation processes personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.
- Processed in accordance with the individual rights under the act
- Personal data should not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Individual Rights

The GDPR includes the following rights for individuals

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object; and
- The right not to be subject to automated decision-making including profiling

Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers.
- for how long their personal data is stored (or how that period is decided).
- their rights to rectification or erasure of data, or to restrict or object to processing.

- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether the organisation conducts automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless they agree otherwise.

If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to hrsupport@briggsmarine.co.uk or use the organisation's form for making a subject access request. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the organisation or causing disruption, or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether it will respond to it.

Consent

The Company tells individuals the reasons for processing their personal data, how it uses it and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the Company relies on its legitimate interests as the basis for processing data, it will conduct an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the Company processes special categories of personal data to perform its obligations or to exercise rights in employment law, this will be done in accordance with a policy on special categories of data.

To ensure we are compliant we will publish and make available our Privacy Statements. We will ensure individuals have received sufficient, specific, and clearly presented information prior to giving consent to the processing of their data.

The organisation will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Individuals have the right to withdraw consent at any time. The Data Controller must inform of this right to withdraw before the consent is given. Where consent has been withdrawn the data, subject can request their personal data be erased.

People, Risks & Responsibilities

This policy applies to:

- The Head Office of Briggs Marine & Environmental Services
- All branches of Briggs Marine Contractors Ltd
- All branches of Briggs Environmental Ltd
- All staff of The Briggs Group
- All contractors, suppliers and other people working on behalf of Briggs Marine

It applies to all data that the Company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR.

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

However, the following people have key areas of responsibility:

Board of Directors

The Board of Directors is responsible for ensuring that The Briggs Group meets its legal obligations

IT Manager

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 instance, cloud computing services

Marketing & Client Relations Manager

The Marketing & Client Relations Manager is responsible for:

- Approving any data protection statements attached to communications such as emails and letters

HR Operations Manager

The HR Operations Manager is responsible for:

- Ensuring the personal data collected, stored, amended, disclosed and or destroyed pertaining to job applicants, employees and ex-employees is in keeping with our Policies and Procedures
- Keeping the Board updated about data protection responsibilities, risks and issues pertaining to employee, ex-employee, or Job applicant personal data
- Reviewing all data protection procedures and related policies in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data that The Briggs Group holds about them (also called a Subject Access Request)
- Checking and approving any contracts or agreements with third parties that may handle sensitive data

- Ensuring Privacy Statements pertaining to Recruitment, Employment and Medical are reviewed and updated in accordance with the Regulations

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Department Heads

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it.

These guidelines also apply to electronically stored data that has been printed:

- 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, for instance a printer, desktop, or meeting room
- 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 removable media (like a CD, DVD, or memory stick), these should be securely locked away when not being used
- Data should only be stored in drives on designated servers and should only be uploaded to a Company 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 and those backups should be tested 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 Breaches

We have a responsibility under The Regulations to report certain data breaches to the Information Commissioner's Office (ICO) within 72 hours of discovery where it is likely to result in a risk to the rights and freedoms of individuals. The organisation will record all data breaches regardless of their effect. Notification must also be given to those individuals concerned.

Examples include:

- Damage to reputation
- Financial Loss
- Loss of confidentiality or any other significant economic or social disadvantage

Data Security

Briggs Group takes the security of personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Where the Company engages third parties to process personal data on its behalf, such parties do so based upon written instructions, and or individual consent and are under a duty of confidentiality and are obliged to implement appropriate technical organisational measures to ensure the security of data.

Individual Responsibilities

Individuals are responsible for helping the company keep their personal data up to date. Individuals should let the company know if data provided to the company changes, for example if an individual moves house or changes their bank details.

Individuals who have access to personal data

Individuals may have access to personal data of other individuals during their employment contract. Where this is the case, the company relies on individuals to meet its data protection obligations to staff.

General Staff Guidelines

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes.
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation.

- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to [name of individual/the data protection officer] immediately.
- Data should not be shared informally, when access to confidential information is required, employees can request it from their line managers
- 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 securely
- Employees should request help from their line manager or the Data Protection Officers if they are unsure about any aspect of data protection

Training

The company will provide training to all individuals about their data protection responsibilities as part of the induction process and whenever new regulations are put in force or amended

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.