UK GDPR Act 2018

Background

The UK GDPR 2018 works alongside the Data Protection Act 2018 as did the EU GDPR before it. Many of the UK GDPR's main concepts and principles are the same.

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.

Data Protection Law

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

- Personal data be processed fairly and lawfully
- Data should be obtained only for one or more specified and lawful purposes
- The data should be adequate, relevant, and not excessive

- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the individual rights under the act
- Data should be kept secure
- 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

The UK GDPR includes the right of access to personal data (SAR) for more information please refer to our **Subject Access Request Policy and Procedure.**

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 carry out 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.

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:

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

- 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

- The Marketing Manager is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters

- The Group HR 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) where it is likely to result in a risk to the rights and freedoms of individuals. 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 move to a new house, 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

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally, when access to confidential information is required, employees can request it from their line managers
- The Briggs Group will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure by taking sensible precautions and following the guidelines below:
    - Strong passwords must be used and should never be shared
    - Personal data should not be disclosed to unauthorised people, either within the Company or externally
    - 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.

Collieson Briggs
Managing Director
Briggs Marine and Environmental Services
March 2022