Privacy Policy

Introduction

B&W Tunnelling Ltd is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of 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.

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 by 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' phone number, email address, educational background, 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 or 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 destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is [the Information Commissioners Office].

Scope

This policy applies to all staff, 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 and guidelines from time to time.

The Principles

B&W Tunnelling shall comply with the principles of data protection in the EU General Data Protection Regulation and the Data Protection Act 2018. We will make every effort possible in everything we do to comply with these principles:

1. Lawful, fair and transparent Data collection must be fair, for a 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.

Privacy Policy

Our Procedures

Fair and lawful processing We must process personal data fairly and lawfully in accordance with individuals' rights.

B&W Tunnelling is classified as a data controller.

Lawful basis for processing data

At least one of the following conditions must apply whenever we process personal data:

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

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

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

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

Public function Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

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.

We will ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This will be in the form of a privacy notice. 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).

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

Privacy 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 through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

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 that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

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.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- 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.

Privacy Policy

Transferring data internationally

There are restrictions on international transfers of personal data. We will not transfer personal data outside the EU.

Rights of individuals

Individuals have rights to their data which we 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 We provide Privacy Notices which are concise, transparent, intelligible and easily accessible, written in clear and plain language. Show how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access Enable individuals to access their personal data and supplementary information. Allow individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification We will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete, without delay, and no later than one month.

4. Right to erasure We will 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 will comply with any request to restrict, block, or otherwise suppress the processing of personal data. We will retain enough data to ensure the right to restriction is respected in the future.

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

7. Right to object We respect the right of an individual to object to data processing based on legitimate interest. We respect the right of an individual to object to direct marketing. We 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 respect the rights of individuals in relation to automated decision making and profiling.

9. Right to complaint Individuals can complain to the Information Commissioner. Full contact details available at **www.ico.org.uk**

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. B&W Tunnelling has a legal obligation to report any data breaches to the Information Commissioner's Office within 72 hours.

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, and notify those whose data has been breached