Data Protection Policy

Introduction

The Brock Metal Company Ltd (the 'Company'), processes information about individuals (i.e. 'personal data') for business purposes, including employment and HR administration, provision of our services, marketing, and business administration. This includes personal data relating to our staff, customers, suppliers and other third parties.

Compliance with data protection law is essential to ensure that personal data remains safe, our business operations are secure and the rights of individuals are respected. The Company is a 'controller' under data protection law, meaning it decides how and why it uses personal data. This Policy, which may be updated at any time, explains how we comply with data protection law.

It applies to all Company employees and workers, including contractors, agency workers, consultants and directors.

The Board is ultimately responsible for the Company's compliance with data protection law.

What is personal data?

Personal data is information relating to a living individual who can be identified (directly or indirectly) by reference to an identifier (e.g. name, NI number, employee number, email address, physical features). This includes colleagues, customers, members of the public, business contacts, etc. Personal data can be factual (e.g. contact details or date of birth), an opinion about a person's behaviour, or information that may otherwise impact on that individual. It may be automated (e.g. electronic records such as computer files or in emails) or manual records either already filed or intended to be filed.

'Processing' personal data means any activity that involves the use of personal data (e.g. obtaining, recording or holding the data, amending, retrieving, using, disclosing, sharing, erasing or destroying). It also includes sending or transferring personal data to third parties.

Data Protection Obligations

Set out below are key obligations and details of how the Company complies with data protection law.

1. Processing personal data in a fair, lawful and transparent manner

Legal grounds for processing
We process personal data only where there are legal grounds to do so.

Examples of legal grounds for processing personal data include the following (at least one of these must be satisfied for each processing activity):

- complying with a legal obligation (e.g. health and safety or tax laws);
- entering into or performing a contract with the individual (e.g. an employee's terms and conditions of employment, or a contract for services with an individual customer);
- acting in the Company's or a third party's legitimate interests (e.g. maintaining records of business activities, monitoring business productivity); and
- obtaining the consent of the individual (e.g. for direct marketing communications).

Where consent is relied upon, it must be freely given, specific, informed and unambiguous, and the Company must effectively demonstrate that consent has been given.

In most cases, consent is not required for normal business activities involving customer or supplier data, but it may be needed for other activities such as direct marketing activities.

Transparency
We are required to process personal data in a transparent way by providing appropriate, clear and concise information about how we process personal data.

2. Sensitive or special categories of personal data

Some categories of personal data are 'special' because they are particularly sensitive. These include information that reveals details of an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- sexual life or sexual orientation;
- biometric or genetic data (if used to identify that individual); and
- criminal offences or convictions.

Where special category personal data is concerned, we must have (as well as one of the legal grounds described in section 1), an additional legal ground to justify using this sensitive information. The appropriate legal ground will depend on the circumstances, and include:

- complying with a legal obligation/exercising a legal right in the field of employment;
- assessing working capacity (based on expert medical opinion, and subject to obligations of confidentiality);
- carrying out equalities monitoring in relation to racial or ethnic origin, religious beliefs, health or sexual orientation;
- exercising, establishing or defending legal claims;
- preventing or detecting unlawful acts; or
- explicit consent of the individual. (As well as the requirements for consent outlined in section 1 above, this requires an express statement from the individual that their special category of data may be used for the intended purposes.)

3. Processing personal data for specified, explicit and legitimate purposes

The Company will only process personal data in accordance with our legitimate purposes to carry out business operations and administer employment and other business relationships.

4. Personal data must be adequate, relevant and limited to what is necessary for legitimate purposes

Data protection law requires that personal data is adequate, relevant to our purposes and limited to what is necessary.

Data Protection Policy

5. Keeping personal data accurate and up-to-date

The Company takes steps to ensure that personal data is accurate and up-to-date. For example, we request that employees provide us with any change in contact details or personal information. We also take care that decisions impacting individuals are based on accurate and up-to-date information.

6. Keeping personal data for no longer than is necessary

Records containing personal data should only be kept for as long as they are needed. The Company has a data retention policy regarding Company records contain personal data.

We take steps to retain personal data only for as long as is necessary, taking into account:

- the amount, nature, and sensitivity of the personal data;
- the risk of harm from unauthorised use or disclosure;
- the purposes for which we process the personal data;
- how long the personal data is likely to remain accurate and up-to-date;
- how long the personal data might be relevant to possible future legal claims; and
- legal, accounting, reporting or regulatory requirements.

7. Measures to keep personal data secure

Keeping personal data safe and complying with the Company's procedures to protect the confidentiality of personal data is a key responsibility for the Company and its workforce.

Measures to achieve this include physical, technological and organisational controls, e.g. locked offices and filing cabinets, building security, access controls and passwords, encryption of hardware or software, anti-virus and network protection, software updates, security testing and incident management, secure disposal of records, backup and disaster recovery.

8. Care when sharing or disclosing personal data

The sharing or disclosure of personal data is a type of processing, and therefore all the principles described in this Policy need to be applied.

Internal data sharing
The Company ensures that personal data is only shared internally on a 'need to know' basis.

External data sharing
We will only share personal data with third parties where we have a legitimate purpose, and an appropriate legal ground. Commonly, this includes situations where we are legally obliged to provide the information (e.g. to HMRC for tax purposes) or to perform our contractual duties to individuals (e.g. provision of information to our occupational pension providers).

We may appoint third party service providers ('processors') who handle information on our behalf, for example to provide payroll, data storage or other services.

The Company is responsible for ensuring that its processors comply with data protection law in handling personal data. We must assess and apply data protection and information security measures prior to and during the appointment of a processor.

Data Protection Policy

9. Transferring personal data to another country

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed, accessed or otherwise processed in, a different country. European Union data protection law restricts personal data transfers outside of the European Economic Area (EEA – the European Union plus Norway, Liechtenstein and Iceland), to ensure that the level of data protection is not compromised (Such countries may not provide the same protection for personal data as the EEA).

To ensure that data protection is not compromised when personal data is transferred to another country, the Company assesses the risks of any transfer of personal data outside of the UK (taking into account the principles in this Policy, as well as restrictions on transfers outside the EEA) and puts in place additional appropriate safeguards where required.

We do not currently transfer personal data outside the UK.

10. Reporting data protection breaches

The Company takes data protection breaches very seriously. These can include lost or mislaid equipment or data, use of inaccurate or excessive data, failure to address an individual's rights, accidental sending of data to the wrong person, unauthorised access to, use of, or disclosure of data, deliberate attacks on the Company's systems or theft of records, and any equivalent breaches by the Company's service providers.

Where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to individuals' personal data, the Company will take immediate steps to identify, assess and address it, including containing the risks, remedying the breach, and notifying appropriate parties.

If the Company discovers that there has been a personal data security breach that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner's Office (ICO) within 72 hours of discovery.

We also keep an internal record of all personal data breaches regardless of their effect and whether or not we report them to the ICO.

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

11. Integrating data protection into operations

Data protection law requires the Company to build data protection considerations and security measures into all of our operations that involve the processing of personal data, particularly at the start of a new project or activity which may impact on the privacy of individuals. This involves taking into account various factors including:

- the risks posed by the processing for the rights and freedoms of individuals;
- technological capabilities;
- the cost of implementation; and
- the nature, scope, context and purposes of the processing of personal data.

Data Protection Policy

Individual Rights and Requests

Under data protection law, individuals have certain rights when it comes to how we handle their personal data. For example, an individual has the following rights:

- **The right to make a 'subject access request'.** This entitles an individual to receive a copy of the personal data we hold about them, together with information about how and why we process it and other rights which they have (as outlined below). This enables them, for example, to check we are lawfully processing their data and to correct any inaccuracies.
- **The right to request that we correct incomplete or inaccurate** personal data that we hold about them.
- **The right to withdraw any consent** which they have given.
- **The right to request that we delete or remove** personal data that we hold about them where there is no good reason for us continuing to process it. Individuals also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (see below).
- **The right to object to our processing** of their personal data for direct marketing purposes, or where we are relying on our legitimate interest (or those of a third party), where we cannot show a compelling reason to continue the processing.
- **The right to request that we restrict our processing** of their personal data. This enables individuals to ask us to suspend the processing of personal data about them, for example if they want us to establish its accuracy or the reason for processing it.
- **The right to request that we transfer** to them or another party, in a structured format, their personal data which they have provided to us. The applicability of this right depends on the legal grounds on which we process it.

We are required to comply with these rights without undue delay and, in respect of certain rights, within a one month timeframe.

Individuals also have rights to complain to the ICO about, and to take action in court to enforce their rights and seek compensation for damage suffered from, any breaches.

Record Keeping

In order to comply, and demonstrate our compliance, with data protection law, the Company keeps various records of our data processing activities. These include a Record of Processing which contains, as a minimum: the purposes of processing; categories of data subjects and personal data; categories of recipients of disclosures of data; information about international data transfers; envisaged retention periods; general descriptions of security measures applied; and certain additional details for special category data.