Data Protection Policy

Introduction

At The Brock Metal Company Ltd (the 'Company'), we process 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 explains how we comply with data protection law.

This Policy does not give contractual rights to Employees, and may be updated at any time.

To whom does this Policy apply?

It applies to all Company employees and workers, including contractors, agency workers, consultants and directors, together referred to as 'Employees' or 'you'.

Who is responsible for data protection at the Company?

The Board is ultimately responsible for the Company's compliance with data protection law. The Health, Safety and Environment Manager advises on compliance with data protection law.

All Employees have responsibility for ensuring that personal data is kept secure and processed in a lawful manner although some have particular responsibilities.

If you have any concerns or questions in relation to this Policy, you should seek advice from your Manager or the Health, Safety & Environment Manager.

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 can be personal or business related.

Personal data 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.

What is 'processing' of personal data?

'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 Policy

Data Protection Obligations

To ensure that the Company meets its responsibilities, it is essential that its Employees comply with data protection law when processing personal data. Set out below are key obligations and details of how the Company expects you to comply.

1. Process 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.

The Company does **not** use consent as a legal ground for processing Employee data unless the data processing activities concerned are genuinely optional.

(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 individuals with appropriate, clear and concise information about how we process their personal data.

We usually provide individuals with basic information about how we use their data on forms which collect data (such as application forms or website forms), and in longer privacy notices setting out details including: the types of personal data that we hold about them, how we use it, our legal grounds for processing the information, who we might share it with and how long we keep it for.

We supplement these notices, where appropriate, with reminders or additional information at the time particular processing activities take place or become relevant for an individual.

What you need to do:

By processing personal data only in accordance with your lawful job duties and Company instructions you will normally be processing personal data lawfully.

Any new forms which collect personal data and any proposed consent wording must be approved in advance by the Health, Safety & Environment Manager. If you have any concerns about the legal grounds for processing personal data or if you are unsure whether individuals have been provided with appropriate information (in particular in relation to any new processing activities), please check with the Health, Safety & Environment Manager.

2. Take extra care when handling 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.)

What you need to do:

If you are handling special category personal data, you need to take extra care regarding compliance with data protection law. In particular, try to ensure that:

- any processing activities are in accordance with your lawful job duties;
- there are appropriate legal grounds for processing the data, assessed for your specific activities;
- individuals have received adequate information regarding how their data is being handled. An existing privacy notice may need to be supplemented with more specific information regarding special category data (e.g. when the Company is managing sickness absence and/or making adjustments to job duties for Employees with disabilities or serious illness, we may provide ad hoc privacy notices);
- you apply additional security and confidentiality measures, taking into account that the impact of misuse of their data may be greater than with other data; and
- if you are relying on consent as a legal ground for processing, you obtain advance approval of any consent wording from the Health, Safety & Environment Manager.

If alternative circumstances apply (e.g. you are involved in a new project or updating an existing system with new types of processing data), contact the Health, Safety & Environment Manager.

3. Only process 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.

What you need to do:

You must only use the personal data that you process in the course of your duties for the Company's legitimate purposes. You must not process personal data for purposes unrelated to your job duties.

Processing personal data for unauthorised purposes could result in a breach of data protection law (e.g. using Company data to find a colleague's home address for non-work related purposes). This may have potentially damaging consequences for all parties concerned, including disciplinary action.

If you find that you need to process personal data for a different purpose from that for which it was originally collected, you must check whether the individual has been informed and, if not, consider whether the additional purpose is legitimate. If you are unsure, contact the Health, Safety & Environment Manager before going ahead with processing the data.

4. Make sure that personal data is adequate, relevant and limited to what is necessary for your legitimate purposes

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

What you need to do:

Ensure that you only process personal data that you need for legitimate purposes, and that you have sufficient personal data to use it fairly and take into account all relevant details.

5. Keep 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.

What you need to do:

When you process personal data you must make reasonable efforts to be accurate and keep the relevant information updated.

When collecting personal data, try to confirm its accuracy at the outset. If you subsequently discover inaccuracies, these need to be corrected or deleted without delay.

Personal data should be held in as few places as possible to avoid the risk that copies are not updated. Do not create additional copies, but work from a central copy where possible.

Data Protection Policy

6. Keep 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.

What you need to do:

Familiarise yourself with our retention policy, and destroy or erase all information that you no longer require. If you are unsure what retention guidelines apply in your role, or of how to apply them, please contact the Health, Safety & Environment Manager.

7. Take appropriate steps 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.

The Company Handbook includes an Electronic Communications Policy and a Social Media Policy with protocols for Employees using our technology and communications systems, which help to ensure appropriate security of personal data.

What you need to do:

To maintain data security and protect the confidentiality of personal data, you must:

- *process personal data only using authorised Company systems.*
- *use password-protected and encrypted software for the transmission and receipt of emails*
- *lock files in a secure cabinet*
- *never leave your laptop, other device or any hard copies of documents containing personal data on public display or in a public place*
- *take care when using personal data in hard copy or on-screen that it is not viewed by anyone without the right to that information, especially if you are in a public place*
- *ensure personal data on portable devices are encrypted and password protected*
- *ensure that personal data is disposed of securely and permanently*
- *alert your Manager or the Health, Safety & Environment Manager to any personal data breaches immediately*

8. Take extra 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.

What you need to do:

You may only share or disclose personal data internally with an Employee, agent or representative of the Company if the recipient has a job-related need to know the information.

You may only disclose personal data to service providers or other third parties where:

- there is a legitimate purpose and an appropriate legal ground for doing so (e.g. it is necessary for them to process the personal data in order to provide a service to us such as payroll, or if we are legally obliged to do so);
- the individuals whose personal data is being shared have been informed (e.g. in a privacy notice);
- if the disclosure is to a service provider, the Company has checked that adequate security and data protection measures are in place to protect the personal data concerned;
- the service provider or third party has signed up to a written contract that contains the provisions required by data protection law; and
- the transfer complies with any overseas transfer restrictions, if applicable.

Routine disclosure of personal data to established recipients as a regular part of your job duties normally satisfies the above. However, if you are in any doubt as to whether you can share personal data, contact your Manager or the Health, Safety & Environment Manager.

9. Do not transfer personal data to another country unless there are appropriate safeguards in place

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.

What you need to do:

If you are required to transfer individuals' personal data outside of the UK or EEA in the course of your employment, adequate safeguards will need to be in place. Where these overseas transfers are a normal part of your role and job duties, the Company's current safeguards are likely to provide the required levels of data protection.

However, if you are transferring personal data overseas in alternative circumstances (e.g. for new types of processing activities which haven't previously formed part of your job scope and activities, or to countries with which you haven't previously dealt) you should contact your Manager or the Health, Safety & Environment Manager before doing the transfer.

10. Report data protection breaches without delay

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.

What you need to do:

If you become aware of any breach (or suspected breach) of this Policy, you must report it to your Manager or the Health, Safety & Environment Manager immediately.

11. Integrate 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.

What you need to do:

If you are involved in the design or implementation of a new project or activity that involves processing personal data, you must give due consideration to the principles of data protection set out in this policy.

A useful tool for assessing data protection and privacy considerations is a Data Protection Impact Assessment or 'DPIA'. A DPIA will consider the necessity and proportionality of a processing operation, and assess the risks to individuals and the measures that can be put in place to mitigate those risks. A DPIA must be carried out if a data processing operation is likely to give rise to a high risk to individual rights and freedoms.

If you are involved in the design or implementation of a new project that involves processing personal data, you must check whether it is necessary to conduct a DPIA or similar risk or compliance assessment by contacting the Health, Safety & Environment Manager.

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.

What you need to do:

If you receive a request from an individual seeking to exercise a right in relation to their personal data, or making an enquiry or complaint about our use of their personal data, you must forward the request, enquiry or complaint to your Manager or the Health, Safety & Environment Manager immediately so that it can be dealt with appropriately and within the applicable time limit.

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 must contain, 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.

What you need to do:

You must also comply with our applicable processes/guidelines and any specific instructions you are given concerning the keeping of records about our processing of personal data.

If you process individuals' personal data in the course of your employment and you collect any new types of personal data or undertake any new types of processing activities, either through the introduction of new systems or technology or by amending existing ones, please inform the Health, Safety & Environment Manager so that we are able to keep our records up-to-date.

Training

Training is provided as part of our induction process for new joiners to the Company along with ongoing training to make sure that Employees' knowledge and understanding for compliance in the context of their role is up-to-date. Attendance at such training is mandatory and will be recorded.