Data Protection Policy

1. Introduction

The Bri-Stor Group consists of Bri-Stor Systems Ltd, Alpha Manufacturing Hixon Ltd and Atlas Coating Ltd. For the purposes of this policy the business will be referred to as "The Bri-Stor Group".

The Bri-Stor Group needs to collect and use certain types of information about job applicants and staff; and the Individuals or Service Users who come into contact with the business in order to carry on our work. This personal information must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under data protection legislation.

2. Definition of data protection terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with data protection legislation.

Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers or contractors which handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings, genetic data and biometric data where processed to uniquely identify a person (for example a photo in an electronic passport). Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3. Data Controller

The Bri-Stor Group is the Data Controller under data protection legislation, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

4. Disclosure

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

We may also disclose personal data we hold to third parties:

In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

We may also share personal data we hold with selected third parties for the purposes set out in the Schedule.

5. Data Protection Principles

The Bri-Stor Group regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

To this end, The Bri-Stor Group will adhere to the Principles of Data Protection, as detailed in data protection legislation.

Specifically, the Principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met

b) Shall be obtained only for one or more of the purposes specified in the legislation, and shall not be processed in any manner incompatible with that purpose or those purposes

c) Shall be adequate, relevant and limited to what is necessary in relation to those purpose(s) (data minimisation)

d) Shall be accurate and, where necessary, kept up to date

e) Shall not be kept for longer than is necessary

f) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information

Furthermore any data processed by the company shall be processed in accordance with the rights of data subjects under data protection legislation.

6. Fair and lawful processing

Data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in legislation. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

7. Specified, explicit and legitimate purposes

In the course of our business, we may collect and process the personal data set out in the Schedule. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by data protection legislation. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

8. Notifying data subjects

If we collect personal data directly from data subjects, we will inform them about their rights under data protection legislation including:

(a) The purpose or purposes for which we intend to process that personal data and the legal basis for the processing.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data including the right to object to processing.

(d) The right of subject access.

(e) The right to be forgotten.

(f) The right to withdraw consent, where processing is based on consent.

(g) The right to rectification if data is inaccurate or incomplete.

(h) Rights related to automated decision making and profiling.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

9. Data minimisation

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

10. Data Storage and Security

Information and records relating to individuals and service users will be stored securely and will only be accessible to authorised staff.

Information will be stored for only as long as it is needed having regard to the purpose it was obtained in the first place and will be disposed of appropriately and securely.

It is The Bri-Stor Group's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

If there is a data security breach which will result in a risk to the data subject we will report that breach to the regulator without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

> **Confidentiality** means that only people who are authorised to use the data can access it.
>
> **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
>
> **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:

> **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
>
> **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
>
> **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

11. Data accuracy

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

12. Processing in line with data Subject's rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them.
- Object to processing, including in particular to prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

13. Transferring personal data to a country outside the EEA

We will only transfer any personal data we hold to a country outside the European Economic Area ("EEA") where the conditions of transfer provided for in data protection legislation apply.

14. Dealing with subject access requests

Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to their line manager immediately.

Our employees will refer a request to their line manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

In addition, The Bri-Stor Group

will ensure that:

- Everyone processing personal information understands that they are responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it holds, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to data protection legislation.

A P Humphrey
Group Managing Director
15th May 2018

Schedule - Data Processing Activities

Type of data	Purpose of processing	Type of recipient to whom personal data is transferred	Retention period
Application Form	To determine suitability for employment	HR, relevant managers and, on occasion, professional advisers	Kept securely until 36 months after either rejection for employment; or the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Correspondence with or about you	For the purposes of the employment relationship, for example, training opportunities, salary reviews	HR, relevant managers and, on occasion, professional advisers.	Kept securely until 36 months after either rejection for employment; or the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Records of holiday, sickness and other absence	Necessary for the purposes of the employment relationship.	HR, relevant managers, HMRC and, on occasion, professional advisers.	Kept securely until 36 months after employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Training records	Necessary for the purposes of the employment relationship	HR, relevant managers and, on occasion, professional advisers.	Kept securely until 36 months after either rejection for employment; or the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Disciplinary and grievance records	Necessary for the purposes of the employment relationship	HR, relevant managers and, on occasion, professional advisers.	Kept securely until 36 months after the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Health and safety records	Necessary for compliance with the legal obligation to protect health and safety at work	HR, Health and Safety Manager, relevant managers, HSE and, on occasion, professional advisers.	Kept securely until 6 years after the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Contract of Employment	Necessary for the purposes of the employment relationship and complying with the legal obligation to provide a written statement of terms of employment.	HR, relevant managers and, on occasion, professional advisers.	Kept securely until 36 months after the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.

Information needed to pay you (e.g. NI number and bank details)	Necessary for the purposes of the employment relationship	HR, HMRC, Payroll, relevant managers and, on occasion, professional advisers.	Kept securely until 6 years after the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Emergency contact details	Necessary for the purposes of the employment relationship	HR, Health and Safety manager and other relevant managers	Discarded once employment ends.
Employment references	To determine suitability for employment	HR, relevant managers and, on occasion, professional advisers	Kept securely until 36 months after either rejection for employment; or the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Career history	To determine suitability for employment	HR, relevant managers and, on occasion, professional advisers	Kept securely until 36 months after either rejection for employment; or the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Performance records	Necessary for the purposes of the employment relationship	HR, relevant managers and, on occasion, professional advisers.	Kept securely until 36 months after the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Evidence of your right to work/ID	To determine legal ability to work in the UK	HR, UK Immigration Authorities, relevant managers and, on occasion, professional advisers.	Kept securely until 36 months after the employment ends, then discarded, unless required for the purposes of defending legal action, in which case maintained for as long as is necessary for that purpose.
Driver details (address, phone number)	To enable delivery and collection of vehicles directly with a customer's employee	Relevant managers, Bri-Stor employed drivers, 3rd party drivers/logistics providers	Kept securely until 72 months after delivery of the goods.
Contact details of customers and their employees	For new business prospecting and ongoing customer relationship management	Relevant managers and employees	Kept until the end of the customer relationship or until a request for amendment or deletion is received.

Security Measures: All data will be kept in a locked filing cabinet and secure IT system. Accessed on a need to know basis only. Further information regarding IT security can be found in the IT Security Policy policy.