

# Data Protection Policy

This policy is applicable to all employees at BDR Group that process personal data.

## Background

BDR Group mission is to be a market leader in the recycling of redundant IT equipment in the UK. In achieving this mission and, as part of the daily operation, BDR Group takes the protection of the personal data it processes extremely seriously. They commit to taking reasonable and proportionate measures to ensure that they protect personal data against accidental or deliberate misuse, damage or destruction. They are also committed to a policy of protecting the rights and freedoms of individuals, in relation to the processing of their personal data, in compliance with the UK Data Protection Legislation.

## Purpose

The purpose of the policy is to ensure all employees comply with the provisions of UK data legislation when processing personal data. A serious breach of the Data Protection Act may result in the company being held liable in law.

This policy applies regardless of where the personal data is held or whether it is held manually or electronically.

## Introduction

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 employees understand the rules governing their use of personal data to which they have access in the course of their work.

## Definitions

Term	Definition
<p><b>Business Purposes</b></p>	<p>The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and sales and business development purposes.</p> <p>Business purposes include the following:</p> <ul style="list-style-type: none"> <li>• Compliance with our legal, regulatory and corporate governance obligations and good practice.</li> <li>• Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests.</li> <li>• Ensuring business policies are adhered to (such as policies covering email and internet use).</li> <li>• Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information.</li> <li>• Supplier information.</li> <li>• Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments.</li> <li>• Monitoring staff conduct, disciplinary matters.</li> <li>• Sales and Marketing of our business.</li> <li>• Improving services.</li> </ul>
<p><b>Personal Data</b></p>	<p>Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.</p> <p>Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and copies of any relevant curriculum vitae.</p>
<p><b>Sensitive Personal Data</b></p>	<p>Personal data about an individual's physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.</p>

## Principles

BDR Group adheres to the principles of both the current UK Data Protection Act and the General Data Protection Regulation. In accordance with these principles personal data shall be:

<b>Data Protection Act 1998</b>	<b>General Data Protection Regulation 2018</b>
Processed fairly and lawfully	Processed lawfully, fairly and in a transparent manner in relation to individuals
Processed for specified purposes only	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes not considered to be incompatible with the initial purposes
Adequate, relevant and not excessive	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accurate and up to date	Accurate and, where necessary, kept up to date; whilst having regard to the purposes for which data is processed, every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
Not kept longer than necessary	Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
Processed in accordance with data subjects' rights	GDPR does not contain a specific principle relating to individuals' rights - these are specifically addressed in separate articles (see GDPR Chapter 3).

Data Protection Act 1998	General Data Protection Regulation 2018
Processed and held securely	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Not transferred outside the countries of the European Economic Area with adequate protection	GDPR does not contain a specific principle relating to overseas transfers of personal data - these are specifically addressed in separate articles (see GDPR Chapter 5).

In addition, the GDPR introduces an ‘accountability’ principle, this ensures that Data Controllers are responsible for, and can demonstrate and verify their compliance with personal data legislation.

## Our Procedures

### Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals’ rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

### The Data Protection Officer’s responsibilities:

- Keeping employees updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all employees and those included in this policy
- Answering questions on data protection from employees
- Responding to individuals such as clients and employees who wish to know which data is being held on them.
- Checking and approving with third parties that handle the company’s data any contracts or agreement regarding data processing

### The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

### Sensitive Personal Data

In most cases where we process sensitive 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). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

### **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 Data Protection Officer.

### **Data Security**

BDR Group will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

### **Storing Data Securely**

- In cases when data is stored on printed paper, it will 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 locked away securely when they are not being used
- The DPO and a Director must approve any cloud used to store data
- Data should be regularly securely backed up
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

### **Subject Access Requests**

Under the Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them. BDR Group may receive a subject access request, this will be referred to the DPO.

### **Training**

All staff will receive training on this policy. New employees will receive training as part of the induction process. Further training will be provided whenever there is a substantial change in the law or our policy and procedure. Completion of training is compulsory.

### **Reporting Breaches**


Employees 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
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

### Consequences of Failing to Comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Signature:		Position:	Managing Director
Name:	Malek Rahimi	Date:	24.01.2024