T 01946 595 200
E info@discoverbec.com
W DiscoverBEC.com

BEC
The Old Board of Trade Building,
High Street, Cleator Moor, CA25 5AH

Data Protection Policy

Introduction

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. This Data Protection Policy sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties, in line with the General Data Protection Regulations 2018 (GDPR). This Data Protection Policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action up to and including summary dismissal.

Definitions

‘’**Automated Decision-Making (ADM**)’’: when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.]

‘’Automated Processing’’: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.]

"**Company Personnel**": all employees, workers [contractors, agency workers, consultants,] directors, members and others.

"**Criminal records data**" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

"**Data Subject**" is a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

‘’Explicit Consent’’: consent which requires a very clear and specific statement (that is, not just action).

"**Personal Data**" is any information that relates to a Data Subject who can be identified from that information, whether directly or indirectly.

"**Processing**" is any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

"**Special categories of personal data**" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Our Nominated Person responsible for data protection

The Nominated Person is responsible for overseeing this Data Protection Policy and, as applicable, developing any related policies and guidelines. That post is held by Rebecca Nicholson, Finance Accountant, 01946 595255,rebecca.nicholson@discoverbec.com. Please contact Rebecca with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed.

Data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the General Data Protection Regulations (GDPR) which require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;
- collected only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purposes of processing;
- accurate and where necessary kept up to date takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- kept only for the period necessary for processing; and
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage and not transferred to another country without appropriate safeguards being in place
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data

Processing Data in a Lawful and Fair manner
You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;
(b) the Processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations;
(d) to protect the Data Subject's vital interests;
(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

You must identify and document the legal ground being relied on for each Processing activity.

Consent
Please note that the rules relating to consent may not apply to certain processing activities. Please speak to the Nominated Person if you are seeking to rely on consent to collect and use Personal Data in the course of your duties.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Categories of Personal Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

Please keep evidence of all consents captured so that the Company can demonstrate compliance with consent requirements.

Informing Data Subjects about what Data we collect and what we use it for (Transparency)
The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects about what Personal Data is being collected, what it is used for and the lawful basis for using it for that purpose. This information is provided in a Privacy Notice.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and nominated person, how and why we will use, Process, disclose, protect and retain that Personal Data through a privacy notice. The privacy notice must be provided to the Data Subject when the Personal Data is collected.

When Personal Data is collected from a third party, you must check it was collected by the third party in accordance with the GDPR and on the basis that it could be shared with us.

Personal Data must be collected only for a specified purpose.
If the Personal Data is to be used for a different purpose to that for which it was originally collected, the Data Subject must be informed beforehand with an explanation of what our lawful basis is for using it for the different purpose. This will usually mean providing an updated privacy notice. If the lawful basis will be consent, fresh consent will be needed from the Data Subject.

Only collect Personal Data necessary for the purpose it is needed for
You must only collect Personal Data that is required for your job duties. Please ensure that when the Personal Data is no longer needed for the specific purposes of your job, it is deleted in accordance with our Data Retention Policy.

Keep Personal Data accurate, complete, up to date and relevant for the purpose it was collected for
You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Do not keep Personal Data for longer than the purpose it was originally collected
Please refer to our Data Retention Policy which explains how long we should be storing Personal Data for and when it should be deleted. Please ensure you take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our Data Retention Policy. You will also need to ask third parties who we have shared that Personal Data to delete it.

Data Subject Rights

Data subject access requests
All Data Subjects have the right to make a subject access request. All subject access requests should be immediately sent to nominated person.

Data Subjects' Additional rights
Data Subjects also have the following rights in relation to how we handle their personal data:

- Right to receive certain information about our how we use their Personal Data
- Right to ask us to rectify data which is inaccurate or incomplete;
- Right to require us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed
- Right to restrict processing in specific circumstances;
- Right to ask us to transfer their Personal Data to a third party;
- Right to object Processing in certain circumstances;
- Right to prevent our use of their Personal Data for direct marketing purposes;
- Right not to be subject to automated decision making
- Make a complaint to the Information Commissioner's Office.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

Sharing Personal Data with third Parties

Generally, you should only share Personal Data with third parties if certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our associated companies if the recipient has a job-related need to know the information. Please refer to the section on international data transfers if the Personal Data is being transferred out of the UK.

You may only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the privacy notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Retention Periods
Personal Data should only be retained for the period necessary, and for the purpose for which it is held. Please see our Data Retention Policy for further information.

Data Security
The Company takes the security of all personal data seriously and adopts appropriate measures to ensure that all personal data is secure, is protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

All individuals who may process personal data on behalf of the Company are required to strictly adhere to its policies and procedures from the point of collection to the point of destruction. We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

You may only transfer Personal Data to third-party service providers, such as payroll providers, pension scheme providers, who agree to comply with our instructions concerning the collection and use of Personal Data which will include having adequate security measures in place to protect the Personal Data.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data. This means you must ensure:

- only people who have a need to know and are authorised to use the Personal Data can access it.
- the Personal Data is accurate and suitable for the purpose for which it is processed.
- authorised users are only able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of this policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

Where the Company uses a third party supplier to process personal data on its behalf, a payroll bureau for example, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data Protection Impact Assessments (DPIAs)
Where Processing may result in a high risk to individual's rights and freedoms, the Company must carry out a DPIA. A DPIA is a tool used to identify and reduce risks of a data processing activity.

Examples of situations which require a DPIA include:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- [Automated Processing including profiling and Automated Decision Making];
- large scale Processing of Special Categories of Personal Data; and
- large scale, systematic monitoring of a publicly accessible area.

Please speak to Nominated Person if you believe a DPIA is necessary.

Reporting a Data Breach
A breach of the data protection regulations or failure to adhere to the Company's policies could have serious repercussions for both the Company and for any individual who is Processing Personal Data on its behalf.

Any breach or suspected breach **must** immediately be reported to your manager and/or the Appointed Person. Do not attempt to investigate the matter yourself. A data breach is any act or failure to act which results in the loss, unauthorised access, disclosure or acquisition of Personal Data. Examples of data breaches include **but are not limited to** losing your laptop, USB stick or mobile phone, leaving documents/files on public transport or sending an email containing Personal Data to the wrong recipient.

The Company will keep a record of all data breaches and, if legally required to do so, will report certain data breaches to the Information Commissioners Office (ICO), and in some circumstances, the Data Subjects.

Any breach or failure to report a breach in a timely manner will be investigated and managed in line with the appropriate procedures. Significant or deliberate breaches of this policy, such as accessing and/or sharing employee or customer data without authorisation or without a legitimate reason to do so may constitute gross misconduct and could result in your summary dismissal.

Training
The organisation will provide training to all individuals regarding their responsibilities under the GDPR as part of their induction process, and refresh regularly thereafter.

Individuals whose roles require access to and/or processing of personal data will receive additional training to ensure a thorough understanding of this policy and associated documents.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Record keeping
The GDPR requires us to keep full and accurate records of all our data Processing activities.
You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO/Nominated Person, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above

Changes to this Data Protection Policy
We reserve the right to change this Data Protection Policy at any time without notice to you.