Data Protection Policy

1. Introduction

1.1 Be Data Solutions Limited (the "Company") holds personal data about job applicants, employees, consultants, clients, suppliers and other individuals for a variety of business purposes.

1.2 This policy sets out how the Company seeks to protect personal data and ensure staff understand the rules governing their use of personal data.

1.3 In particular, this policy requires staff to ensure that the Company's Data Privacy Manager should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed, including carry out a privacy impact assessment and security review.

1.4 The Company's Data Protection Officer is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy or other comments you should contact Keith Bishop, Chief Technical Officer.

2. Scope

2.1 This policy applies to all staff, which for these purposes includes employees, consultants, temporary and agency workers, other contractors, interns and volunteers.

2.2 All staff must be familiar with this policy and comply with its terms.

2.3 This policy supplements any other Company policies from time to time in force relating to information security, document management and retention, deletion, procurement and communications.

2.4 This policy does not form part of any terms and conditions of employment Company may supplement, amend or withdraw this policy at any time.

3. Definitions

3.1 In this policy:

Business purposes: means the purposes for which personal data may be used by the Company, eg personnel, administrative, financial, regulatory, payroll and business development purposes;

Personal data: means information relating to identifiable individuals, such as job applicants, current and former employees, consultants, agency, contract and other staff, clients, suppliers and marketing contacts. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual, and unique identifier such as IP addresses;

(Special category) sensitive personal data: means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexual life. It includes genetic and biometric data. Criminal offences, or related proceedings are treated in a similar way to sensitive data. Any use of sensitive personal data must be strictly controlled in accordance with this policy;

Processing data: means obtaining, recording, holding or doing anything with data, such as organising, using, altering, retrieving, disclosing or deleting it.

4. General principles

4.1 The Company's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All staff have personal responsibility for the practical application of the Company's data protection policy.

4.2 The Company will observe the following principles in respect of the processing of personal data:

4.2.1 to process personal data fairly, lawfully, transparently and in line with individuals' rights;

4.2.2 to make sure that any personal data processed for a specific, explicit and legitimate purpose are only processed for that purpose and as per instructions from the employer. The data processed should be adequate, relevant and limited to what is needed for that purpose; records to be maintained of the purpose and legal grounds of processing;

4.2.3 to keep personal data accurate and where needed up to date; reasonable steps to be taken to delete or rectify personal data that is inaccurate for its purpose;

4.2.4 to keep personal data for no longer than is necessary;

4.2.5 to process data in a way that ensure that we maintain security of the data against unauthorised or unlawful processing and against accidental loss, destruction or damage;

4.2.6 not to transfer personal data outside the EEA (which includes the EU countries, Norway, Iceland and Liechtenstein) without adequate protection, or such arrangements as required as a result of withdrawal from the European Union;

4.2.7 to cooperate with investigations, audits and assisting the Data Protection Officer with carrying out data subject rights requests;

4.2.8 when appropriate to your role, assist with the maintenance of data inventories.

5. Security

5.1 Staff must keep personal data secure against loss, destruction or misuse in accordance with this policy. Where the Company uses external organisations to process personal data on its behalf additional security arrangements should be implemented in contracts with those organisations to safeguard the security of personal data. Staff should consult the Company's Data Protection Officer to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

5.2 Staff must ensure any data transferred within the organisation or to third parties is done so securely and in accordance with this policy.

6. Data retention and Management

6.1 Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances including the reasons why the personal data was obtained. It is also important to label and store personal data in accordance with any applicable data management procedures for security and compliance with deletion policies and subject rights.

7. International transfer

7.1 Staff should not transfer personal data internationally without first consulting the Company's Data Protection Officer. Transfer includes hosting. There are restrictions on international transfers of personal data to other countries because of the need to ensure adequate safeguards are in place to protect the personal data. Staff unsure of what arrangements have been or need to be put in place to address this requirement should contact the Company's Data Protection Officer.

8. Rights of individuals

8.1 Individuals have a number of rights, such as to request access to information held about them, right to be forgotten and objecting to direct marketing. All such requests or complaints should be referred immediately to the Company's Data Protection Officer. This is particularly important because the Company must respond to a valid request within the legally prescribed time limits. You should also assist with any requests made of you in relation to your job role by the Company's Data Protection Officer to comply with data subject rights such as if you are asked to carry out a search for personal data.

8.2 Any member of staff who would like to correct or request information that the Company holds relating to them should contact the Company's Data Protection Officer. It should be noted that there are certain restrictions on the information to which individuals are entitled under applicable law.

8.3 Staff should not send direct marketing material to someone electronically (eg by email or SMS) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the Data Protection Officer about any such request. Staff should contact the Company's Data Protection Officer for advice on direct marketing before starting any new direct marketing activity.

9. Reporting breaches

9.1 Staff have an obligation to report actual or potential data protection compliance failures to the Company's Data Protection Officer as soon as possible. This allows the Company to:

9.1.1 investigate the failure and take remedial steps if necessary; and

9.1.2 make any applicable notifications.

10. Consequences of failing to comply

10.1 The Company takes compliance with this policy very seriously. Failure to comply puts both staff and the Company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

10.2 Staff with any questions or concerns about anything in this policy should not hesitate to discuss these with the Company's Data Protection Officer.

11. How we deal with subject access requests

11.1 We must provide an individual with a copy of the information requested, free of charge. This must occur without delay, and within one month of receipt. We endeavor to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.\If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the Data Protection Officer before extending the deadline.

11.2 We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the Data Protection Officer.

11.3 Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

12. Data portability requests

12.1 We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the Data Protection Officer first.

13. Right to erasure

13.1 What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed;

- Where consent is withdrawn;
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed or otherwise breached data protection laws;
- To comply with a legal obligation;
- The processing relates to a child;
- How we deal with the right to erasure;
- We can only refuse to comply with a right to erasure in the following circumstances:
    - To exercise the right of freedom of expression and information
    - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
    - For public health purposes in the public interest
    - For archiving purposes in the public interest, scientific research, historical research or statistical purposes
    - The exercise or defense of legal claims

13.2 If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

14. <u>The right to object</u>

14.1 Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defense of legal claims.

14.2 We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

15. <u>The right to restrict automated profiling or decision making</u>

15.1 We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

16. <u>Third parties</u>

16.1 Using third party controllers and processors

- As a data processor, we must have written contracts in place with any third-party data controllers (and/or) data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.
- As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

17. <u>Contracts</u>

17.1 Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers (and/or) data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions;
- Those involved in processing the data are subject to a duty of confidence;
- Appropriate measures will be taken to ensure the security of the processing;
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract;

- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR;
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments;
- Delete or return all personal data at the end of the contract;
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations;
- Nothing will be done by either the controller or processor to infringe on GDPR.

18. Criminal offence data

18.1 Criminal record checks.

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the Data Protection Officer prior to carrying out a criminal record check.

19. Audits, monitoring and training

19.1 Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the Data Protection Officer and normal procedures.

19.2 Monitoring

Everyone must observe this policy. The Data Protection Officer has overall responsibility for this policy. You must notify the Data Protection Officer of any breaches of this policy. You must comply with this policy fully and at all times

19.3 Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move roles or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the Data Protection Officer.

20. <u>Reporting breaches</u>

20.1 Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. We have a legal obligation to report any data breaches to the Information Commissioner's Office within 72 hours.

20.2 All members of staff 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;

20.3 Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

21. <u>Failure to comply</u>

21.1 We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

21.2 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.

21.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer, Keith Bishop.