cititectalent

Data Protection Policy

CITITEC TALENT LIMITED ("the Company")
Version 3 (October 2022)

INTRODUCTION

All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the retained EU law version of the General Data Protection Regulation (EU) 2016/679 (UK GDPR) and the Data Protection Act 1998 (or its successor legislation) (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their *personal data* whilst imposing certain obligations on the organisations that process their data.

As a recruitment business, the Company collects and processes both *personal data* and *sensitive personal data*, including data about the company personnel. It is required to do so to conduct its business and comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how the Company ('we', 'our', 'us') collects, processes and protects personal data and implements the Data Protection Laws. It should be read in conjunction with the Privacy Notice.

This policy applies to all company personnel ('you', 'your'). You must read, understand and comply with this policy when processing personal data on our behalf.

DEFINITIONS

In this policy the following terms have the following meanings:

'company personnel' means all employees, workers, contractors, agency workers, consultants, directors, members and others.

'***consent***' means any freely given, specific, informed and unambiguous indication of a data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of persona data relating to him or her;

'***data controller***' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*. The Company is the data controller of all personal data relating to our company personnel and personal data used in our business for our own commercial purposes;

'***data processor***' means an individual or organisation which processes *personal data* on behalf of the *data controller*;

'data subject' means a living, identified or identifiable individual about whom we hold personal data;

'***personal data***'* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'*personal data breach*' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*;

'*processing*' means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'*profiling*' means 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 natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'*sensitive personal data*'* means *personal data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions; and

'*Supervisory authority*' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Office (ICO).

The Company processes *personal data* in relation to company personnel, work-seekers and individual client contacts and is a *data controller* for the purposes of the Data Protection Laws.

1. Collecting personal data

We may collect, use, store and otherwise process the following non-exhaustive list of information:

- Personal name and contact details;
- Emergency contact details;
- Personal bank details; and
- Employment history and qualifications.

We may collect, use, store and otherwise process sensitive data such as details of health-related information or criminal offence data when the data subject provides such information. This category of information is only processed with the data subject's prior consent (and unless otherwise permitted under the law to process such data) and will be handled with a higher degree of protection at all times. Examples of when we might need to process sensitive data include when we are acting as your employer and we require such information to comply with our legal and regulatory requirements (such as to verify your right to work and identity) or to provide you with various benefits such as statutory sick pay or to enrol you in a pension scheme where applicable.

The Company may hold *personal data* on individuals for the following purposes:

- Staff administration;
- Advertising and marketing;
- Accounts and records;

- Administration and *processing* of work-seekers' *personal data* for the purposes of providing work-finding services, including *processing* using software solution providers and back office support; and
- Administration and *processing* of clients' *personal data* for the purposes of supplying/introducing work-seekers.

2. The data protection principles

The Data Protection Laws require the Company acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that *personal data* that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the *personal data* are processed;
6. 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;
7. Made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data; and that
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

3. Legal basis for processing

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Company will only process *personal data* where it has a legal basis for doing so. Where the Company does not have a legal reason for *processing personal data* any processing will be a breach of the Data Protection Laws.

The UK GDPR allows us to process your *personal data* for specific purposes, and the bases on which we will primarily rely are set out below:

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject;
- To meet our legal compliance obligations;
- To pursue our legitimate interest for purposes where they are not overridden because the processing prejudices the interests of fundamental rights and freedoms of data subjects.

The Company will review the *personal data* it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring *personal data* to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), the Company will establish that (i) it has a legal reason for making the transfer under the UK GDPR, or (ii) the UK has issued regulations confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subject's rights and freedoms, or (iii) appropriate safeguards are in place (such as use of special contractual documentation known as the International Data Transfer Agreement (IDTA) or the UK Addendum which have been issued and approved by the UK Government and the ICO).

4. Privacy by design and by default

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities. This includes implementing measures such as:

- data minimisation (i.e. not keeping data for longer than is necessary);
- cyber security;
- privacy impact assessments where necessary;
- staff training on Phishing;
- encryption on all mobile devices;
- banning of USB memory sticks.

The Company shall provide any information relating to data *processing* to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

5. Privacy notices

Where the Company collects personal data from a data subject, the Company will give the data subject a privacy notice at the time before collecting the personal data.

Where the Company collects personal data other than from the data subject directly, it will give the data subject a privacy notice within a reasonable period of collecting the personal data, but at the latest within one month.

Where the Company intends to further process the personal data for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further processing.

6. Data subjects' rights and requests

A data subject has rights when it comes to how we handle their personal data. These include rights to:

- Withdraw consent to processing at any time;

- Receive certain information about the controller's processing activities; and
- Request access to their personal data;
- Ask us to rectify inaccurate data or to complete incomplete data.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the *personal data* unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold – however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

- **Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed;**

The data subject or another *data controller* at the data subject's request, has the right to ask the Company to erase a data subject's *personal data.*

If the Company receives a request to erase it will ask the data subject if s/he wants his/her *personal data* to be removed entirely or whether s/he is happy for his or her details to be kept on a list of data subjects who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of data subjects whose data it has erased so the data subject may be contacted again by the Company, should the Company come into possession of the data subject's *personal data* at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other *data controllers* and *data processors processing* the *personal data* to erase the *personal data*, taking into account available technology and the cost of implementation.

If the Company has given the *personal data* to any third parties it will tell those third parties that it has received a request to erase the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold – however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

- **Ask us to restrict our use of their personal data**

The data subject or a *data controller* at the data subject's request, has the right to ask the Company to restrict its *processing* of a data subject's *personal data* where:

- The data subject challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the data subject opposes its erasure;
- The Company no longer needs the *personal data* for the purposes of the *processing*, but the *personal data* is required for the establishment, exercise or defence of legal claims; or
- The data subject has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the data subject.

If the Company has given the *personal data* to any third parties it will tell those third parties that it has received a request to restrict the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold – however

the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

- **Ask to receive personal data concerning them (data portability)**

The data subject shall have the right to receive *personal data* concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *data controller* in circumstances where:

- The *processing* is based on the data subject's *consent* or a contract; and
- The *processing* is carried out by automated means.

Where feasible, the Company will send the *personal data* to a named third party on the data subject's request.

- Object to *processing*

The data subject has the right to object to their *personal data* being processed based on a public interest or a legitimate interest. The data subject will also be able to object to the *profiling* of their data based on a public interest or a legitimate interest.

The Company shall cease *processing* unless it has compelling legitimate grounds to continue to process the *personal data* which override the data subject's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The data subject has the right to object to their *personal data* for direct marketing.

7. Enforcement of rights

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision-making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature, the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved, provided the data subject is informed of such refusal or charging of fees.

8. Automated decision making

The Company will not subject data subjects to decisions based on automated *processing* that produce a legal effect or a similarly significant effect on the data subject, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the *data controller* and the data subject;
- Is authorised by law; or
- The data subject has given their explicit *consent*.

The Company will not carry out any automated decision-making or *profiling* using the *personal data* of a child.

9. Reporting personal data breaches

All data breaches should be referred to the persons whose details are listed in the Appendix.

a. *Personal data breaches* where the Company is the *data controller*:

Where the Company establishes that a *personal data breach* has taken place, the Company will take steps to contain and recover the breach.

The UK GDPR requires controllers to notify any personal data breach to the UK Information Commissioner (ICO) and, in certain instances, the data subject. Where the *personal data breach* happens outside the UK, controllers shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

We have put in place procedures to deal with any suspected personal data breach and will notify the data subject or any applicable regulator where we are legally required to do so.

b. *Personal data breaches* where the Company is the *data processor*:

The Company will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

10. Complaints

If you have a complaint or suggestion about the Company's handling of *personal data* then please contact the person whose details are listed in the Appendix to this policy.

Alternatively you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

APPENDIX

Data Protection Officer:
Ben Iddon
+44 (0) 20 7608 5854
dpo@cititec.com