THEORISE

Westpoint, 4 Redheughs Rigg, Edinburgh, EH12 9DQ

0131 589 2363

www.theoriseltd.com

Data Protection Policy

Contents

Introduction

All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act 2018 (or its successor) and the UK General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their *personal data* while imposing certain obligations on the organisations that process their data.

As a recruitment business the Company collects and processes both *personal data* and *special categories of personal data*. In some cases, it is required to do so to 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 implements the Data Protection Laws. It should be read in conjunction with the Data Protection Procedure.

In this policy the following terms have the following meanings:

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

'*data controller*': means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data;

'*data processor*': means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'data subject'†: means the identified or identifiable living individual to whom personal data;

'*personal data*'*: means any information relating to an identified or identifiable natural persona ('data subject'); an identifiable natural persona is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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* transmitted, stored or otherwise processed;

'*processing*': means any operation or set of operations which is performed on *personal data* or on sets of *personal data*, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption 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 a natural person, 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;

'*pseudonymisation*': means the *processing* of *personal data* in such a manner that the *personal data* can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable natural person;

'*special categories of personal data*'*: means the processing of 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 for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

† For the purposes of this policy we have used the term 'individual' to mean '*data subject*'.

* For the purposes of this policy we use the term '*personal data*' to include '*special categories of personal data*' except where we specifically need to refer to *special categories of personal data*.

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

The Company processes *personal data* in relation to its own staff, work-seekers, individual college / university contacts and the students we area assigned to work and is a *data controller* for the purposes of the Data Protection Laws. The Company has registered with the ICO, and its registration number is **ZA430867.**

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

- Staff administration;
- Advertising, marketing and public relations
- 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;
- Administration and *processing* of clients' *personal data* for the purposes of supplying/introducing work-seekers
- Students we are referred to whom we provide support to via colleges and universities via non-medical personal help support. The basis for the support provided to students with a disability, health condition or specific learning difficulty is determined partly by legal requirements (The Equality Act 2010) but also by the College or University's standards, strategy and values which incorporate being 'inclusive'.

1. 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, explicit 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, where necessary, kept up to date; every reasonable step must be taken to ensure that *personal data* that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the *personal data* is 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; and
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the data protection principles.

2. Legal bases for processing

The Company will only process *personal data* where it has a legal basis for doing so (see Annex A). 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 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. Those people listed in page 10 shall be responsible for doing this.

Before transferring *personal data* to any third party (such as past, current or prospective employers, staff, suppliers, colleges and universities, students 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 it has a lawful reason for making the transfer.

3. 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);
- *pseudonymisation*;
- anonymisation
- cyber security

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.

1. Privacy notices

Where the Company collects *personal data* from the individual, the Company will give the individual a privacy notice at the time when it first obtains the *personal data*.

Where the Company collects *personal data* other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the *personal data*, or at the time it contacts the individual, but at the latest within one month. If the Company intends to disclose the *personal data* to a third party, then the privacy notice will be issued when the *personal data* are first disclosed (if not issued sooner).

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*.

2. Subject access requests

The individual is entitled to access their *personal data* on request from the *data controller*.

3. Rectification

The individual or another *data controller* at the individual's request, has the right to ask the Company to rectify any inaccurate or incomplete *personal data* concerning an individual.

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. If asked to, the Company must also inform the individual about these recipients. 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.

4. Erasure

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

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

5. Restriction of processing

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

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes its erasure but requests restriction instead;
- The Company no longer needs the *personal data* for the purposes of the *processing*, but the individual needs the Company to keep the *personal data* in order to establish, exercise or defend a legal claim; or
- The individual 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 individual.

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. If asked to, the Company must also inform the individual about these recipients. 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.

6. Data portability

The individual 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 individual's *consent* or a contract; and
- The *processing* is carried out by automated means (i.e. excluding paper files).

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

7. Object to processing

The individual has the right to object to their *personal data* being processed based on a public interest, the exercise of official authority vested in you, or a legitimate interest (or those of a third party).

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

8. Enforcement of rights

All requests regarding individual rights should be sent to the person(s) whose details are listed in page 10.

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. The Company will let the individual know within one month of receiving his or her request and explain why the extension is necessary.

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.

9. Automated decision making

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

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

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

Reporting *personal data* breaches

All data breaches should be referred to the persons whose details are listed in page 10.

1. 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. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO, and where necessary, the individual/s concerned.

Where the *personal data breach* happens outside the UK, the Company shall alert the relevant authority for data breaches in the effected jurisdiction.

2. 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.

3. Communicating personal data breaches to individuals

Where the Company has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

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/

Names of those responsible for:

- adding, amending or deleting *personal data*;
- responding to subject access requests/requests for rectification, erasure, restriction, data portability, objection and automated decision making processes and profiling;
- reporting data breaches/dealing with complaints:

- Dany Brunton, Director, dany@theoriseltd.com – Main point of contact
- Angela Brunton, Director, angela@theoriseltd.com
- Monika McMorrine, Administrator, monika@theoriseltd.com

a) The lawfulness of *processing* conditions for *personal data* are:

1. ***Consent:*** *the individual has given clear consent for you to process their personal data for a specific purpose.*
2. ***Contract:*** *the processing is necessary for the performance of a contract with the data subject or in order to take specific steps before entering into a contract.*
3. ***Legal obligation:*** *the processing is necessary for compliance with a legal obligation to which the data controller/data processor is subject to.*
4. ***Vital interests:*** *the processing is necessary to protect someone's life.*
5. ***Public task:*** *the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official functions, and the task or function has a clear basis in law.*
6. ***Legitimate interests:*** *the processing is necessary for the legitimate interests pursued by the data controller or a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.*

b) The lawfulness of *processing* conditions for *special categories of personal data* are:

1. The *data subject* has given explicit consent to the *processing* of the *special categories of personal data* for one or more specified purposes, except where the *data subject* is not permitted or able to give *consent*.
2. *Processing* is necessary for carrying out obligations and exercising specific rights of the *data controller* or of the *data subject* under employment, social security or social protection law, in so far as it is authorised by UK law or a collective agreement, provided for appropriate safeguards for the fundamental rights and interests of the *data subject*.
3. *Processing* is necessary to protect the vital interests of the *data subject* or another person where the *data subject* is physically or legally incapable of giving *consent*.
4. *Processing* is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the *personal data* are not disclosed outside that body without the consent of the *data subject*(s).
5. *Processing* relates to *personal data* which manifestly made public by the *data subject*.
6. *Processing* is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
7. *Processing* is necessary for reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject domestic law.
8. *Processing* is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of UK law or a contract with a health professional and subject to relevant conditions and safeguards.
9. *Processing* is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices on the basis of UK law.
10. *Processing* is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the *data subject*.