Company Name:	Thrive Recruitment Limited ("the Company")
Policy Name:	Information Security and Data Protection
Date:	12/04/23
Version:	1.0

The Data Protection Act 1998

The Company processes personal data in relation to its own staff, work-seekers and individual client contacts - therefore it is a "*data controller*" for the purposes of the Data Protection Act 1998 & GDPR. The Company has notified the Information Commissioner's Office – the Company's data protection registration number is ZA312821.

The Company holds personal data on individuals ("*data subjects*") for the following general purposes:

- Staff administration
- Provide advice and services as an Employment Agency
- Advertising, marketing and public relations.
- Accounts and records
- Administration and processing of work-seekers personal data for the purposes of work-finding services.

The eight principles of data protection

The Data Protection Act 1998 requires the Company as data controller to process data in accordance with the principles of data protection. These require that personal data shall be:

1. Fairly and lawfully processed.
2. Processed for limited purposes.
3. Adequate, relevant and not excessive.
4. Accurate.
5. Not kept longer than necessary.
6. Processed in accordance with the data subjects rights.
7. Kept securely.
8. Not transferred to countries outside the European Economic Area without adequate protection.

"*Personal data*" means data, which relates to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of the Company.

"*Processing*" means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data, which does not amount to processing. It applies to any processing that is carried out on computer including any type of computer however described, main frame, desktop, laptop, iPad, Blackberry ® or other mobile device.

Personal data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Personal data may only be processed with the consent of the person whose data is held. Therefore if they have not consented to their personal details being passed to a third party this may constitute a breach of the Data Protection Act 1998. By instructing the Company to look for work and by providing us with personal data contained in a CV work-seekers will be giving their consent to processing their

details for work-finding purposes. If you intend to use their personal data for any other purpose you MUST obtain their specific consent.

Caution should be exercised before forwarding the personal details of any individuals on whompersonal data is held, to any third party such as past, current or prospective employers, suppliers, customers and clients, persons making an enquiry or complaint and any other third party.

Sensitive personal data

Personal data in respect of the following is "*sensitive personal data*" and any information held on any of these matters MUST NOT be passed on to any third party without the express written consent of the individual:

- Any offence committed or alleged to be committed by them.
- Proceedings in relation to any offence and any sentence passed.
- Physical or mental health or condition.
- Racial or ethnic origins.
- Sexual life.
- Political opinions.
- Religious beliefs or beliefs of a similar nature.
- Whether someone is a member of a trade union.

Information security

From a security point of view, only those staff listed in the Appendix are permitted to add, amend or delete personal data from the Company's database(s) ("database" includes paper records or records stored electronically). However all staff are responsible for notifying those listed where information is known to be old, inaccurate or out of date. In addition all employees should ensure that adequate security measures are in place. For example:

- Computer screens should not be left open by individuals who have access to personal data.
- Passwords should not be disclosed.
- Computer records should be encrypted or password protected
- Email should be used with care.
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason.
- Personnel files should always be locked away when not in use and when in use should not be left unattended.
- Any breaches of security should be treated as a disciplinary issue.
- Care should be taken when sending personal data in internal or external mail.
- Destroying or disposing of personal data counts as processing. Therefore care should be taken in the disposal of any personal data to ensure that it is appropriate. Such material should be shredded or stored as confidential waste awaiting safe destruction.

It should be remembered that the incorrect processing of personal data e.g. sending an individual's details to the wrong person, allowing unauthorised persons access to personal data, or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/or negligence leading to a claim against the Company for damages from an employee, work-seeker or client contact. **A failure to observe the contents of this policy will be treated as a disciplinary offence.**

The rights of the Individual under GDPR

1. the right to withdraw consent;
2. the right to be informed;
3. the right to data portability;
4. the right to object;
5. rights in relation to automated decision making and profiling;
6. the right to rectification of incorrect or incomplete data; and
7. the right to erasure (the right to be 'forgotten');

Privacy/transparency information to be provided to data subjects

The GDPR obliges data controllers to provide specific information to data subjects when first collecting their personal data. For recruitment businesses, this information should be included in your privacy notices when first obtaining personal data from candidates.

The GDPR covers two scenarios:

1. when personal data is obtained directly from the data subject; and
2. when personal data is not obtained directly from the data subject.

(1) Personal data obtained directly from data subject

Where data is obtained directly from the data subject then, the following information should be provided:

1. the identity and contact details of the controller and the controller's representative where applicable;
2. the contact details of the data protection officer where applicable;
3. the purposes and legal basis for processing;
4. the legitimate interest pursued by the controller or by a third party (if legal basis is a legitimate interest);
5. the recipients or categories of recipients of personal data;
6. details of transfers to third countries and safeguards;
7. retention period and criteria used to determine this;
8. existence of the data subject's rights under the GDPR;2199
9. the existence of the right to withdraw consent if relying on this basis;
10. the right to lodge a complaint with a supervisory authority;
11. the existence of automated decision-making, including profiling, as well as the logic involved and predicted consequences of such processing for the data subject; and
12. whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract, whether the data subject is thus obliged to provide their personal data and the possible consequences of such a failure.

(2) Personal data not obtained directly from data subject

Where data is not obtained directly from the data subject then all of the above information should be provided **(except the last bullet point above)** but with two additional pieces of information below:

1. the source from which the personal data originates, and whether it came from a publicly accessible source; and
2. the categories of personal data concerned.

Where the personal data is collected from the data subject s/he should receive the transparency information at the time the personal data is collected.

Where the personal data is not collected from the data subject, the transparency information should be provided no later than one month after the data was collected, or at the time of the first communication from the data controller to the data subject if that is before one month expires. Similarly, if the personal data is to be disclosed to a third party and that disclosure happens before the one month expires, then the information must be provided no later than the first disclosure.

Subject access requests

Data subjects are entitled to obtain access to their data on request. All requests to access personal data by data subjects should be referred to Thrive Recruitment's designated data controller who's contact details can be found in the Appendix.

References

Any requests for access to a reference given by a third party must be referred to Thrive Recruitment's designated data controller and should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with the Data Protection Act 1998, and not disclosed without their consent. Therefore when taking up references an individual should always be asked to give their consent to the disclosure of the reference to a third party and/or the individual who is the subject of the reference if they make a subject access request. However if they do not consent then consideration should be given as to whether the details of the individual giving the reference can be deleted so that they cannot be identified from the content of the letter. If so the reference may be disclosed in an anonymised form.

The Human Rights Act 1998

Finally it should be remembered that all individuals have the following rights under the Human Rights Act 1998 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, conscience and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Freedom from discrimination (Article 14).

APPENDIX

Contact details for Thrive Recruitment's designated data controller who is responsible for adding, amending or deleting data, and responding to subject access requests:

Email: security@thriverecruitment.co.uk
Telephone: 0161 823 3495