DATA PROTECTION POLICY

General Data Protection Regulations (GDPR)

Introduction

At RE Resource Group, we collect and process information about individuals (i.e., 'personal data') for business purposes, including employment and HR administration, provision of our services, marketing and business administration. This includes personal data relating to our staff, customers, suppliers and other third parties.

Compliance with data protection law is essential to ensure that personal data remains safe, our business operations are secure, and the rights of individuals are respected. RE Resource Group is a controller under data protection law, meaning it decides how and why it uses personal data. This policy sets out how the Company implements the Data Protection Laws in relation to personal data. It should be read in conjunction with the **Data Protection Procedure**.

As a recruitment business, the Company collects and processes both personal data and sensitive personal data. 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.

There will also be other policies which will impact on how you deal with personal data and data protection, and you should comply with these where relevant.

This policy applies to all employees, workers, consultants, volunteers and apprentices.

Who is responsible for Data Protection?

Teresa Norris is the Data Protection Officer and is the person with responsibility for overseeing, advising and administering compliance with this Policy and data protection law.

All employees also have responsibility for ensuring that personal data is kept secure and processed in a lawful manner.

If you are in any doubt about how you should handle personal data, or if you have any concerns or questions, you should contact Teresa Norris at teresan@reresourcegroup.co.uk.

Why is data protection compliance important?

Data protection law in the UK is regulated and enforced by the Information Commissioner's Office (ICO). Failure to comply with data protection law may expose RE Resource Group and, in some cases, individual employees to serious legal liabilities. These can include criminal offences and fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher. In addition,

an individual may seek damages from us in the courts if we breach their rights under data protection law. Breaches of data protection law will also lead to serious damage to our reputation.

In addition to the legal liabilities, failure to comply with your obligations may lead to disciplinary action and, in serious cases, it could result in the termination of employment.

Definitions

"Consent" means any freely given, specific, informed and unambiguous indication of an individual'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 an individual or organisation which determines the purposes and means of the processing of personal data.

"Data processor" means an individual or organisation which processes personal data on behalf of the data controller.

"Personal data" is any information that relates 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.

"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, biometric data and criminal convictions.

"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.

"Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual 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 individual.

"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).

Data Processing under the Data Protection Law

The Company processes personal data in relation to its own staff, work-seekers and individual client contacts and is a data controller for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration numbers are:-

Re People	ZA053228
RE Personnel	Z1181462
Ambrose	ZA179333
Safehands	ZA042763

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.

The Data Protection Principles

The Company processes personal data in accordance with the following data protection principles:-

1. Processes personal data lawfully, fairly and in a transparent manner.
2. Collects personal data only for specified, explicit and legitimate purposes.
3. Processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
4. Keeps personal data and takes all reasonable steps to ensure the inaccurate personal data is rectified or deleted without delay.
5. Keeps personal data only for the period necessary for processing.
6. Personal data is 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. The data controller is responsible for, and be able to demonstrate, compliance with the principles.

Legal bases for processing

The Company will only process personal data where it has a legal basis for doing so (see attached). 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 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 e.g., software solutions providers and back office support), the Company will establish that it has a legal reason for making the transfer.

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 (ie., not keeping data for longer than necessary)
- Pseudonymisation
- Anonymisation
- Cyber Security

For further information please refer to the **Company's Information Security Policy**

Rights of the Individual

The Company shall provide any information relating to data processing to an individual in a concise, transparent 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.

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, 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.

Subject Access Requests

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

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. 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.

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. 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.

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 an individual's personal data where:

- The individual challenges the accuracy of the personal data;
- The processing is unlawful and the individual 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 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. 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.

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.

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

Object to processing

The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest. The individual 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 individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their personal data for direct marketing. **Please refer to the Company's Marketing Policy for further information.**

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.

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 person whose details are listed in 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. 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.

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

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.

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.

The Company will not be required to tell individuals about the personal data breach where:

- The Company has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

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).

Appendix A

Data Protection Officer

RE Resource Group
7-9 Ambrose Street
Cheltenham
Glos GL50 3QR

Tel. 07725244857/01242 505400

Email – teresan@reresourcegroup.co.uk

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

1. Consent of the individual for one or more specific purposes.
2. Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
3. Processing is necessary for compliance with a legal obligation that the controller is subject to.
4. Processing is necessary to protect the vital interests of the individual or another person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
6. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of personal data, in particular where the individual is a child.

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

1. Explicit consent of the individual for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law.
2. Processing is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
3. Processing is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving consent.
4. In the course of its legitimate activities, processing is carried out 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 only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the consent of the individual.
5. Processing relates to personal data which are manifestly made public by the individual.
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 EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.
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 the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary 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 healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.
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 fundamental rights and interests of the individual.