

Remedy Recruitment Group **Data Protection Policy**

As a recruitment company Remedy Recruitment processes personal data in relation to its own staff, agency workers and individual client contacts. It is of paramount importance that we abide by the principles of the Data Protection Act 1998 set out below.

Remedy Recruitment holds data on individuals for the following general purposes:

- Staff Administration
- Advertising, marketing and public relations
- Accounts and records
- Administration and processing of agency workers personal data for the purposes of work-finding services

The Data Protection Act 1998 requires Remedy Recruitment as data controller to process data in accordance with the principles of data protection. These require that 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, Remedy Recruitment.

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, tablet etc.

Data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date and Remedy Recruitment have designated personnel that shall be responsible for doing this.

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 Remedy Recruitment to seek employment opportunities and providing us with personal data contained in a curriculum vitae, agency workers will be giving

Ref: RemPol19

their consent to processing their details for recruitment purposes. If intended to use their data for any other purpose specific consent must be obtained in writing.

However caution should be exercised before forwarding personal details of any of the individuals on which 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.

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

From a security view point, only those staff approved by Remedy Recruitment should be permitted to add, amend or delete data from the database. 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
- 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.

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 Remedy Recruitment for damages from an employee, agency worker or client contact. A failure to observe the contents of this policy will be treated as a disciplinary offence.

Data subjects, i.e. those on whom personal data is held, are entitled to obtain access to their data on request and may be subject to a fee. All requests to access data by data subjects i.e. staff, members, customers or clients, etc. should be made in writing.

Ref: RemPol19

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]