Data Protection & Information Security Policy

Data Protection

Prospectus 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. Prospectus has notified the Information Commissioner's Office and our data protection registration number is *Z6814085*. It complies with the requirements of the Act with regard to the collection, storage, processing and disclosure of personal information and is committed to upholding the Act's eight core Data Protection Principles (http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles).

Prospectus holds personal data on individuals for the following general purposes:

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

Personal Data

Prospectus Ltd holds personal details on job applicants and temporary workers, including name, address, email address and contact numbers, as well as availability details, skills and work requirements. These details are processed for recruitment purposes and includes processing carried out on computer including any type of device including server, desktop, laptop, tablet or any mobile device. This involves forwarding CVs, job applications, timesheets and references to third party clients. Prospectus also stores payroll details for temporary workers in order to process payroll, and records Equal Opportunities data for monitoring purposes only. Under the Employment Agencies Act, Prospectus is obliged to hold data for twelve months after it was last used. HMRC requires that payroll details are kept for three tax years and invoice related details for six tax years.

Prospectus holds information on organisations including contact names, addresses and telephone numbers. It also stores details about temporary and permanent jobs for recruitment and invoicing purposes. As above, invoice details are kept for six years in compliance with our legal obligations.

Personal data is reviewed on a regular basis to ensure that it is accurate, relevant and up to date and Prospectus employees 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 applying for a job or instructing Prospectus to look for work, 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. Personal data used for any other purpose requires the consent of the person (s).

Caution should be exercised before forwarding the personal details of any individuals on whom personal 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

Sensitive personal data, such as information in respect of criminal convictions, related to a protected characteristic or a health matter for example, must not be passed on to any third party without the express written consent of the individual.

Information security

Prospectus goes to great lengths to protect your data from loss, misuse, unauthorised access or disclosure, alteration, or destruction. Only employees who need the information to perform a specific job are granted access to your information. Prospectus employees are permitted to add, amend or delete personal data from Prospectus's database(s) (paper based and/or electronically). All employees should ensure that adequate security measures are in place. For example:

- Computer screens should be locked when stepping away from desks.
- Prospectus's clear desk policy should be adhered to.
- Passwords only disclosed to relevant staff members when required.
- Email should be used with care ensuring data sent goes to the intended recipient.
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed.
- Personnel files should always be locked away when not in use and when in use should not be left unattended.
- Personal data should be disposed of appropriately – stored safely and then shredded or destroyed.

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 Prospectus 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.

Subject access requests

Individuals are entitled to obtain access to their data on request in writing and after payment of a fee (currently £7.50). All requests to access personal data by individuals, or queries in respect of this policy, should be referred to the Deputy Chief Executive.

Prospectus Ltd
20-22 Stukeley Street,
London, WC2B 5LR

020 7691 1925 (Text Relay Service)
www.prospect-us.co.uk