SRGlegal.co.uk
+44 (0)1892 278 893

Data Protection Policy

The Company is committed to being transparent about how it collects and uses Personal Data and to meeting its data protection obligations. This policy sets out the Company's commitment and your obligations in relation to data protection, and individual rights and obligations in relation to Personal Data.

This Policy sets out how the Company handles the Personal Data of our customers, suppliers, employees, workers and other third parties. This Policy applies to all Personal Data we Process regardless of the media on which Personal Data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Policy applies to all employees, workers, contractors, agency workers, consultants, directors and any others who process Personal Data on behalf of the Company. You must read, understand and comply with this Policy when processing Personal Data on our behalf and attend training on its requirements.

All Directors are responsible for ensuring compliance with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Company has appointed Andrew Stoneham as the person with responsibility for data protection compliance within the Company. Questions about this policy, or requests for further information, should be directed to andrew.stoneham@stonerecruitmentgroup.com

Failure to comply with this Policy will be regarded as serious misconduct and will be dealt with in accordance with the Company's disciplinary policy and procedure.

Definitions:

Personal Data: any information that relates to an individual who can be directly or indirectly identified from that information. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour, or an identification number, online identifier or location data.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding/storing the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Data protection principles

The Company processes Personal Data in accordance with the following data protection principles which require Personal Data to be:

- processed lawfully, fairly and in a transparent manner
- collected only for specified, explicit and legitimate purposes
- processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- accurate and for the company to take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- kept only for the period necessary for the purposes of processing
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

The Company tells individuals the reasons for processing their Personal Data, how it uses such data and the legal basis for processing in its privacy notices. It will not process Personal Data for other reasons.

The Company will update Personal Data promptly if an individual advises that his/her information has changed or is inaccurate.

The Company keeps full and accurate records of its processing activities in respect of Personal Data in accordance with the requirements of data protection legislation.

Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The Company has developed, implemented and maintains safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data.

You are responsible for protecting the Personal Data by adhering to the safeguards we have put in place but you must also take practical steps to ensure against unlawful or unauthorised

processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure. You must comply with all security arrangements in place including information technology, such as password-protected files and screen savers and other organisational arrangements including locks for drawers and filing cabinets and restricted access arrangements.

When Personal Data is destroyed this must be in accordance with secure destruction arrangements. Personal Data must not be thrown into general rubbish bins. Particular care must be taken where it is necessary to take information away from the Company's premises. You should protect against accidental disclosure such as, for example, someone near to you being able to read information over your shoulder.

Never disclose Personal Data to other employees or a third party either orally or in writing without the prior consent of your Manager and until all appropriate checks and contractual arrangements have been made.

Individuals who have access to Personal Data are required:

- to access only Personal Data that they have authority to access and only for authorised purposes necessary for the performance of their role
- not to disclose Personal Data except to individuals (whether inside or outside the Company) who have appropriate authorisation
- to keep Personal Data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction)
- not to remove Personal Data, or devices containing or that can be used to access Personal Data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the Personal Data and the device
- not to store Personal Data on local drives or on personal devices that are used for work purposes

Reporting a Personal Data Breach

Data protection law requires the Company to notify certain Personal Data Breaches to the applicable regulator within 72 hours and, in certain instances, to the individual without undue delay.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact Andrew Stoneham. You should preserve all evidence relating to the potential Personal Data Breach.

Individual rights

Individuals have a number of rights in relation to their Personal Data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

- whether or not his/her Personal Data is processed and if so why, the categories of Personal Data concerned and the source of the Personal Data if it is not collected from the individual
- to whom his/her Personal Data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers
- for how long his/her Personal Data is stored (or how that period is decided)
- his/her rights to rectification or erasure of Personal Data, or to restrict or object to processing
- his/her right to complain to the Information Commissioner if he/she thinks the Company has failed to comply with his/her data protection rights
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making

The Company will also provide the individual with a copy of the Personal Data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, the Company will charge a fee, which will be based on the administrative cost to the Company of providing the additional copies.

To make a subject access request, the individual should send the request to Andrew Stoneham. In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform the individual if it needs to verify his/her identity and the documents it requires.

The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their Personal Data. Under certain circumstances they can require the Company to:

- rectify inaccurate data
- stop processing or erase data that is no longer necessary for the purposes of processing
- stop processing or erase data if the individual's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data)

- stop processing or erase data if processing is unlawful
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Company's legitimate grounds for processing data
- transfer Personal Data to another party where processing is carried out by automated means

To ask the Company to take any of these steps, the individual should send the request to andrew.stoneham@stonerecruitmentgroup.com.

Training and audit

The Company will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to Personal Data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

We will regularly review all the systems and processes in place to ensure proper use and protection of Personal Data.