Data Protection Policy

Employee Data

This is our policy and statement of the purposes for which we hold and process personal data about our candidates (applicants), sub-contractors and freelancers in accordance with our statutory obligations including the EU General Data Protection Regulation (GDPR).

Definitions

"Company" means Scoot Recruit Ltd

"data" means information which is stored either

- electronically (whether on a computer, a removable drive or any other electronic device)
- in a paper-based filing system which is structured and can be browsed by criteria
- regardless of whether that filing system is dispersed across multiple locations

"data controller" means a person who determines the purposes for which, and the manner in which, any personal data is processed, in this case Daniel Marks, Director

"data processor" means a person who processes personal data on behalf of a data controller and does not in any way determine how or why data is processed

"data subject" means a living individual to whom personal data relates

"ICO" means the Information Commissioner's Office, the UK regulator for data protection law

"personal data" means any data relating to a data subject that either is identified in that data or is directly or indirectly identifiable from that data – e.g. only by reference to an identifier such as a name, an identification number, location data, an online identifier or username, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person, regardless of whether that data is fact or opinion

"processing" means any activity that involves use of personal data. It includes, but is not limited to obtaining, recording or holding 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 transferring personal data to third parties

"sensitive personal data" means personal data that:

- reveals the relevant person's race or ethnic origin, political opinions, religious or philosophical beliefs (or beliefs of a similar nature), membership of a trade union
- is genetic data, or biometric data for the purpose of uniquely identifying the relevant person
- concerns the physical health, mental health, sex life or sexual orientation of the relevant person
- relates to the commission or alleged commission of a criminal offence
- relates to proceedings against the relevant person for a criminal offence or alleged criminal offence, including the disposal of those proceedings, or sentencing

"security breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

General

The Company acts as a data controller, which means that during the course of our activities, we will collect, hold and process information consisting of personal data including sensitive personal data about all applicants for employment and sub-contractors who represent Scoot in freelance or contract employment. The information, which may be held on paper, within computer files or on other media is subject to certain legal safeguards in accordance with GDPR and UK domestic legislation.

This policy sets out our rules on data protection and the legal conditions which must be satisfied in relation to any act taken in relation to personal information, including but not limited to the obtaining, handling, processing, storage, transportation and destruction of personal information. Anyone processing personal data on behalf of the Company must only do so as instructed and in accordance with this policy and any other policy or procedure designed to ensure our compliance with our legal obligations.

If you consider that the policy has not been followed in respect of personal information about yourself or others, you should raise the matter with either of the company directors.

Data Protection Principles

Anyone processing personal data must comply with six data protection principles. Those are that personal data must be:

1 Processed lawfully, fairly and in a transparent manner.

This includes a requirement to

- have a "legal basis" for processing personal data
- be transparent with data subjects, providing them specific information about the processing to be carried out before it is carried out and to give data subjects certain rights in relation to their personal data.

When processing personal data, we must

- not use personal data in a way that would have an unjustified adverse effect on the individual
- only handle people's personal data in ways they would reasonably expect
- not do anything unlawful with a person's personal data.

2 Collected for a specific, explicit and legitimate purpose, and not further processed in a manner that is incompatible with those purposes.

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by GDPR or other relevant legislation.

This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose, or there is a new purpose, for which the data is processed, the data subject must be informed of the changed or new purpose before any processing occurs, and you must only use personal data for that changed or new purpose if it is compatible with the existing purpose.

3 Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.
If personal data later becomes excessive in relation to the purpose, it will need to be deleted unless there is another purpose (and associated legal basis) for keeping it.

4 Kept accurate and, where necessary, kept up to date.

Personal data must be accurate and kept up to date. Personal data which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards.
Inaccurate or out-of-date data that cannot be rectified should be destroyed.

5 Kept for no longer than is necessary for the purposes for which it is processed.

Data should be destroyed or erased from our systems when it is no longer required for the purpose originally notified to the data subject.

6 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.

We are must maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with our procedures and policies, or if they put in place adequate measures to ensure data security.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows.

- confidentiality means that only people who are authorised to use the data can access it
- integrity means that personal data should be accurate and suitable for the purpose for which it is processed
- availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on a central database or ATS system instead of individual local files.

In addition, all employees should ensure that adequate security measures are in place. For example

- 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
- 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
- Computer screens should not be left open by individuals who have access to personal data
- Passwords should not be disclosed
- Emails should be used with care
- Care should be taken when sending personal data in internal or external mail

Legal Basis for Processing

Personal data must be processed lawfully, fairly and in a transparent manner.
Under GDPR there must have be legal basis for processing. One such legal basis must apply to our processing of personal data for it to be lawful.

The GDPR allows processing for specific purposes, including

- the data subject has given his or her consent
- the processing is necessary for the performance of a contract with the data subject
- to meet our legal compliance obligations
- to protect the data subject's vital interests
- where the task is carried out in the public interest or in the exercise of official authority
- other than by public authorities to perform their tasks, to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy statements/notices or fair processing notices.

If processing sensitive personal data, more stringent rules apply. These include:

- the data subject has explicitly consented to processing for a specific purpose (explicit consent being a clear statement in words, rather than by action);
- the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the company or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or UK law
- the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

- the processing relates to personal data which are manifestly made public by the data subject
- the processing is necessary for the establishment, exercise or defence of legal claims
- the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of 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 UK law or pursuant to contract with a health professional and subject to certain conditions and safeguards.

Data Subject's Rights and Requests

Data subjects have rights when it comes to how we handle their personal data. These include

- The right to receive a copy of their personal data which the company holds and details of
  - the purpose for processing
  - the categories of data processed
  - any recipients (or categories of recipients) to whom the personal data has been disclosed
  - the envisaged period for processing
  - the existence of the right to request rectification or erasure
  - the source of the information (if not from the data subject themselves)
  - automated decision making, including meaningful information about the logic involved, and the significance and envisaged consequences of such decisions
  - the safeguards put in place if the personal data has been transferred outside the European Economic Area

- The right to complain to the ICO
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

Right to Rectification

We must rectify any inaccurate information held by us at the request of the data subject. This includes having incomplete personal data completed. This does not affect our primary obligation to keep personal data accurate and up-to-date.

Right to Erasure

We must erase personal data at the request of the data subject, but only in limited circumstances, namely where

- the personal data is no longer necessary for the purpose it was processed
- we originally relied on consent, that consent is withdrawn, and we have no other legal basis for processing
- the personal data is unlawfully processed
- the personal data has to be erased for compliance with a legal obligation to which we are subject

Right to Restriction of Processing

We must restrict our processing at the request of the data subject where

- the accuracy of the personal data is contested by the data subject, but only for a period enabling us to verify the accuracy of the personal data
- the processing is unlawful, and the data subject opposed the erasure of the personal data and requests the restriction of their use instead
- we no longer need the personal data for the purposes of processing, but it is required by the data subject for the establishment, exercise or defence of legal claims
- the data subject has objected to processing pursuant to the right to object to legitimate interests processing but only pending the verification of whether our legitimate grounds override those of the data subject (if they do not, we would then have to permanently restrict processing).

Retention of Data

The categories of information which we will hold and the minimum time for which we will normally hold it will be as follows:

Application to be represented by the Company	one year
Financial details/payroll information	five years from end of most recent booking
References	two years
Summary of any employment facilitated by the Company	ten years

Reporting a Personal Data Breach

We may be required to report personal data breaches to the ICO and in certain instances, the data subject.

Human Rights Act 1998

In addition to GDPR, all individuals have the following rights under the Human Rights Act 1998

- 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 of discrimination (Article 14)