DATA PROTECTION POLICY

The company is committed to ensuring that we are fully transparent and accountable for the personal data of our employees including its collection, usage and storage. We are committed to fulfilling our data protection obligations.

This policy is applicable to employees, contractors and former employees.

The company has appointed Caroline Cooper as the responsible person for data protection compliance within the company. If you need to contact her, you can email her at helpdesk@soloservicegroup.com

Definitions

"Personal data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"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 and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

Processing of personal data is required for HR purposes. The following data protection principles are applied to process HR related personal data:

- We process personal data lawfully, fairly and in a transparent manner.
- We collect personal data only for specified, explicit and legitimate purposes.
- We only process personal data where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We take steps to ensure records reflect accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data for the period necessary for processing only.
- We put in place appropriate measures to ensure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

We will always tell individuals the reasons their personal data needs to be processed within our employee privacy notice, including how we use the data and the legal basis the company relies upon to process your data. We will not process your data for any other reason.

Where the company processes criminal records data this is to perform statutory obligations or to exercise rights in employment law.

If an employee informs the company that their information has changed or is inaccurate the company will correct it without delay.

Personal data gathered during the employment, worker, contractor or apprenticeship term is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the company holds HR-related personal data is confirmed in our privacy notice.

We keep records of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have certain rights in relation to their personal data.

Subject access requests

You have the right to make a subject access request. If you make a subject access request, the company will tell you:

- whether or not data is processed and the reasons for processing, the categories of personal data concerned and the source of the data if it was not collected from the individual;
- to whom your data is or may be disclosed, including confirmation as to whether any of the recipients are located outside the European Economic Area (EEA). The company will also confirm the safeguards in place that apply to such transfers;
- how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- about your right to complain to the Information Commissioner if you believe the company has failed to comply with your data protection rights; and
- whether or not automated decision-making or profiling occurs and the reasons for any such decision-making occurring.

The company will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form.

Subject Access Request Process

A request should be emailed to helpdesk@soloservicegroup.com

In some cases, the company may need to ask for proof of identification prior to processing the request; (e.g. in the cases of a former employee requesting information or the request being submitted from an email address that is not detailed on your HR records) you will be informed of this if it is a requirement.

The company will normally respond to the request within one month (30 days) from the date it is received, however, in some cases, for example, where large amounts of personal data is held, the timescales may be extended to three months from the date of the request to ensure the company is able to provide all information requested. The company will ensure you are informed within one month of receiving the original request if this is the case.

Additionally, where a subject access request is manifestly unfounded or excessive, the company is not obliged to comply with it. Alternatively, the company may 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 if it repeats a request the company has already responded to. If an individual submits a request that is unfounded or excessive, the company will inform them that this is the case and whether or not it will respond to it within 14 days of receiving the request.

Other rights

In addition to the right to access, you also have a number of other rights in relation to your personal data. You can request the company:

- corrects inaccurate data;
- stops processing or deletes data that is no longer necessary for the purposes of processing;
- stops processing or deletes data if your interests override the company's legitimate grounds for processing data (if the company relies on its legitimate interests or consent as a reason for processing data, please refer to the employee privacy notice to review the companies legal basis for processing your data);
- stops processing or deletes data if the processing is unlawful; and
- stops processing data for a period of time if the data is inaccurate or there is a dispute about whether or not your interests override the company's legitimate grounds for processing data.

To ask the company to take any of these steps, you should send the request to helpdesk@soloservicegroup.com.

Data security

The company is committed to ensuring there are proper measures and controls in place to ensure the security and safety of HR-related personal data. We do this by having internal policies and controls to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees who require access to allow the proper performance of their duties (e.g. HR department).

Where third parties are contracted to process personal data on behalf of the company, security measures are confirmed in written agreements which also confirm the third parties obligations to confidentiality of any data they process. The company will not use any third parties to process data unless we are satisfied they have appropriate measures, systems and controls in place to protect data.

Impact assessments

The company will complete a data protection impact assessment where processing could result in a high risk to individual's rights and freedoms, This involves considering the purposes for processing data, assessing the risks to employees and what steps can be taken to reduce the risk to the individual.

Data breaches

The company will report within 72 hours to the ICO any data breach involving personal data that is likely to pose a risk to the rights and freedoms of individuals. The company will maintain an internal record of all data breaches regardless of their effect.

If it is determined that a breach is likely to be high risk to individuals involved, the company will inform affected individuals of the breach and provide them with information about possible consequences and the steps taken by the company to mitigate the impact of the breach.

International data transfers

The company may transfer HR related personal data to countries outside the EEA; However on these occasions the company will ensure that any processing is carried out in compliance with the EU-US Privacy Shield Framework

Individual responsibilities

Individuals have a responsibility to assist the company to keep their personal data up to date. You are obliged to inform the company if any of the data we hold about you changes e.g. change of address or banking details.

You may during the course of your employment have access to personal data of employees, applicants, customers, clients or other individuals. Where this occurs you are responsible for assisting the company to fulfil its data protection obligations to these individuals.

Staff with access to personal data are required:

- only to access data that they have authority to access for a specified purpose;
- not to share data with individuals (internally or externally) unless there is authorisation to do so;
- to maintain the security of data and ensure all data protection and security policies and procedures are followed;
- not to take personal data form the company premises without obtaining permission. If permission is granted to remove personal data you must ensure that appropriate security measures are in place and that only approved storage devises are used;
- only to store personal data on shared drives, personal data must not be stored on local or personal drives used for work purposes.

Failing to comply with these rules will be treated as a disciplinary offence, serious or deliberate breaches of this policy may be treated as gross misconduct which may result in dismissal without notice.

Training

The company will provide about data protection during induction. If your role requires regular access to personal data additional training specific to your duties will be provided.