Data Protection Policy

Aim

The protection of Company and personal data is important to the success of our business. This policy sets out the Company's approach to protecting this data and provides a guideline for the lawful handling of personal data.

This policy applies to all employees, contractors and temporary workers.

Definitions

"Personal data" is any information that enables an individual to be identified.

"Data processing" covers a wide range operations performed on personal data by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, alignment or combination, restriction, erasure or destruction.

Our Commitment

The Company is committed to ensuring that personal data, is processed in line with GDPR and UK law and requires all employees to conduct themselves in line with this policy and other related policies. Where third parties process data on behalf of the Company, we will ensure they take appropriate measures in order to maintain the Company's commitment to protecting data.

Data protection principles

All personal data obtained and held by the Company will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant data protection procedures for international transferring of personal data.

Keeping your personal data up to date

We need to ensure your personal data is accurate and up to date. Please tell us if your details change (for example if you move address, bank accounts or change your name).

If you believe that the data the Company holds on you is inaccurate, either as a result of a subject access request or otherwise, please let us know so the Company can take steps to rectify the information.

Keeping Data Safe

To help protect Company and personal data all employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- not send emails containing sensitive work related information or personal data to their personal email address
- regularly check on the accuracy of data being entered into computers
- not share their passwords with anyone
- use computer screen blanking to ensure that data is not left on screen when not in use
- ensure they take appropriate steps to verify the identity of those requesting access data prior to its disclosure.
- not keep data, including emails, longer than required
- report any concerns or incidents concerning data protection or data security immediately to their manager or to the Data Protection Officer.

In addition personal data should not be kept or transported on laptops, USB sticks, or similar devices, unless specifically authorised by their line manager. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left unattended or where they are at risk of being stolen.

Access to data

Individuals have a right to be informed whether the Company processes personal data relating to them and to access that data. Requests for access to this data will be dealt with as follows:

- a form on which to make a subject access request is available from the UK Compliance Officer. The request should be made to *GDPRmanagement@uk.rhenus.com*
- the Company will not charge for this unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- the Company will respond to any request without delay. Access to data will be provided within one month. This may be extended by a further two months where requests are complex or numerous.

Breach notification

Any suspected data security breaches should be promptly reported to the UK Compliance officer. The breaches will be logged, the severity of the breach established and appropriate action taken. Where a data breach is likely to result in a risk to the rights and freedoms of individuals, the affected person(s) will be notified within 72 hours of the Company becoming aware of it. This will also be reported to the Information Commissioner in the same time frame

Accessing your PC

All new employees are required to sign a consent form which gives authority for ALS to access work related information on that individual's computer.

This consent form is available from IT and should be returned when signed.

Records

The Company keeps records of its processing activities, this includes the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

Data Protection Officer

Mike Morris, is the Company's appointed Compliance Officer in respect of its data protection activities. He can be contacted by email, Mike.Morris@uk.rhenus.com

Compliance

Failure to follow the Company's rules on data protection are taken seriously and may be dealt with via the Company's disciplinary procedure. Both the individual employee and the Company may be held liable for breaches of data, this can result in heavy fines and criminal charges being levied.