

12.4 General Data Protection Policy Statement

To ensure compliance with the General Data Protection Regulations (GDPR) the following policy has been written to assist with the required arrangements to be put in place. We must ensure all employees and key personnel are aware of their legal duties and that documents we hold with personnel data is protected in accordance with GDPR. We also need to verify how employee's individual rights including, how information would be deleted.

Under the GDPR we have defined our company as the processor of personal data and understand that we will be in breach if we do not apply our legal duties. We are required to record an array of employee records with regards to health records, to comply with CAR 2012 for the specific purpose of collecting data for personal monitoring and exposure record requirements, which will need to be maintained. This data is collected only for our company use and records and is not shared with any other third party, other than if requested by the HSE for compliance.

This data is already well protected with regards to key paperwork files stored in locked filing cabinet with only designated admin staff requiring access for maintaining records as works progress and documents are updated. The recording of data includes both paperwork based, scanned documents, computer stored documents and data uploaded to our database, all of which is covered by GDPR, and must be protected. Therefore, all employees will be required to assist in our compliance and not share sensitive personal data with others without the permission of the company Data Protection Officer (DPO).

We have appointed a DPO to apply the principles of the roles and responsibilities that this position would require, therefore safe guarding our data records. We are also required to hold Disclosure Barring Service (DBS) records for some of our clients, therefore potentially holding more sensitive data on previous criminal convictions and offences.


All employee's will be required to complete our right to consent for the maintaining of their personnel records to enable us to comply with CAR 2012 requirements initially and at the same time comply with the GDPR. This form will be handled by the DPO to ensure all employees are signed up to this requirement. If employees feel they are not able to give such consent, then they must be referred to the section of the CAR 2012 which requires an employer to record such data and maintain for 40 years.

Our computer-based system is password protected for each individual user, with the DPO having password access override if employee leaves company and passwords requiring changing to prevent access thereafter for that employee. All computer-based documentation is backed up by secure remote location server which the DPO has main access control only. All computer users must set up a screen saver mode to ensure when leaving their desk sensitive personnel information cannot be accessed by others.

All employees that have access to sensitive information will receive internal training on how to assist us with compliance by operating a clear desk policy at the end of each working day and when they will be away from their desk for a long period time, such as a lunch break or visiting site. Those responsible for maintaining lockable cabinets will also be instructed on keeping lock on the cabinets when not in use.

We have conducted an internal information audit map to identify areas of data flow in and out of the company and assessed the possible risks that may breach an individual's rights and the freedom of individuals. This will be reviewed at least 6 monthly, to ensure compliance remains in place and identify any new additional information flows, that may present a risk.

Full details of our compliance will be detailed within our GDPR privacy policy.

Signed: 
Mr. Bradley Rees, Managing Director

Date: 8th August 2018