PRIVACY NOTICE

The privacy notice lays down conditions for the processing of any personal data.

Personal data is defined as any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The Company holds information on Employees, Customers/Clients, Client End Users and Business Contacts.

Collection of Personal Data

The Company may collect and use the following types of personal data about you:

- Contact details such as company name, company contacts, titles, addresses, telephone numbers and email addresses, VAT numbers and bank details.
- Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies.
- Your contact details and date of birth.

Handling of personal and sensitive information

The Company will, through appropriate management and the use of strict criteria and controls: -

- Observe fully the conditions concerning the fair collection and use of personal information.
- Specify the purpose for which information is used.
- Collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements.
- Endeavour always to ensure the quality of information used.
- Not keep information for longer than required operationally or legally.

- Always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment, protecting personal data held on computers and computer systems by the use of secure passwords which, where possible, are changed periodically and ensuring that individual passwords are not easily compromised).
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the lawful rights of people about whom the information is held can be fully exercised.
- There is someone with specific responsibility for data protection in the organisation (the designated Data Protection Officer).

- A clear procedure is in place for anyone wanting to make enquiries about handling personal information, and that such enquiries are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.

Sharing Your Personal Data

We may on occasion share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Access to Personal Data

All individuals with personal data held by the Company are entitled to:

- Ask what information we hold about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Have inaccurate personal data corrected or removed.
- Prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else.
- Require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters.
- Be informed of what we are doing to comply with our obligations under the GDPR (Regulation (EU) 2016/679).

This right is subject to certain exemptions which are set out in the GDPR (Regulation (EU) 2016/679). Any person who wishes to exercise this right should make the request in writing to the Compliance Manager.

We reserve the right to charge the maximum fee payable for each individual access request. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

We aim to comply with requests for access to personal information as quickly as possible and within 1 calendar month of receipt of a verbal or written request, however we can extend this period for up to 3 months from the date the request is received should this be necessary and only after we have notified you.

Personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Anyone who is in doubt regarding an access request should check with the Compliance Manager. Information must under no circumstances be sent outside of the UK without the prior permission of the Director.

Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. We have implemented appropriate physical, technical and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure. In addition we limit access to personal data to those employees, agents, contractors and other third parties that have legitimate business need for such access.

Retention and Disposal of Data

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for personal data, we consider our statutory obligations, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes we process your personal data for, and whether we can achieve those purposes through other means. Under some circumstances we may anonymise your personal data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent. Once you are no longer a customer of the company, we will retain and securely destroy your personal data.

Right to Withdraw Consent

Where you have provided your consent to the collection, processing, or transfer of your personal data, you may have the legal right to withdraw your consent under certain circumstances. To withdraw your consent, if applicable, please contact us.

Implementation, Review and Monitoring of this Data

The Director has overall responsibility for implementing and monitoring this Policy, which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes in legislation or to our working practices.

Any questions or concerns about the interpretation or operation of this Policy should be taken up in the first instance with the Director who is responsible for ensuring compliance with the GDPR (Regulation (EU) 2016/679) and implementation of this Policy.

This Policy is not contractual but indicates how The Company intends to meet its legal responsibilities for data protection. Any breach will be taken seriously and may result in formal disciplinary action.

Any Employee who considers that the Policy has not been followed in respect of personal data about themselves should raise the matter with their Line Manager or the Director.