

Data Protection Policy Statement



The nature of the Company's work means it has always taken the protection of client data very seriously and treats all such data as confidential as a matter of course.

This statement sets out the measures in place to safeguard data and comply with the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR, effective 2021) which are applicable to operations within the UK, and the EU GDPR, for operations within the EU and European Economic Area.

The Company:

- Has procedures in place for handling data.
- Cooperates with external organisations, e.g. clients and suppliers, accommodating their requirements, whilst making sure our own systems are not put at risk.

'Data' includes:

- Client data relating to projects exchanged in the normal course of business.
- Supplier data relating to products and services.
- Personal details for employees (including former employees) and job applicants.
- Data passed to other parties in the normal course of our business, e.g. training companies, medical providers, and governments.
- All 'personal data', as defined in the GDPR.

IT Security

We have secure IT systems to protect against unauthorised access to data. This has been assessed and given Cyber Essentials Plus certification. Our IT security system is continually improved with formal reviews on an annual basis.

Virus protection and other security software applications associated with our IT and web-based systems are supported by specialist suppliers that ensure these are all current. Regular training through 'KnowBe4' ensures employees are up to date with current threats and how to mitigate the risks they pose.

Employees are not permitted to download software to a computer without the prior approval of a system administrator.

Staff Responsibility

The Company has identified those who have access to and use of data. Staff are made aware of their responsibilities and are asked to acknowledge this in writing.

This includes taking appropriate steps to guard against unauthorised access to, alteration, accidental loss, disclosure or destruction of data.

Employee access to the server drives is based on a number of profiles and only access to data relevant to each employees' role is enabled. Any changes in access are only with express permission of the Managing Director. Passwords or other cyber security measures are to be kept confidential.

GDPR

The GDPR places legal requirements on the handling of personal data. The Company satisfies these mandatory requirements through privacy notices, procedures, staff awareness and IT measures.

Email/Internet use:

All employees are asked to be diligent and alert for phishing or other emails that might be carrying viruses or other malware that may try to access data. As with virus and security threats, individuals are sensitised through training via 'KnowBe4' to question the legitimacy of every email received.

Queries or concerns?

If you have any queries or concerns regarding data protection, please contact us. You can find our details on our website www.zetica.com.

A handwritten signature in blue ink, appearing to read "Mike Sainsbury".

Mike Sainsbury
MD, Zetica Ltd

Date: 5th March 2023

A handwritten signature in black ink, appearing to read "Asger Eriksen".

Asger Eriksen
CEO, Zetica Ltd

Date: 5th March 2023