Phoenix STS Ltd
Data Protection Policy v2.0
Review Date: 05/01/2024

Protecting and storing delegate information securely is crucial, especially given the sensitive nature of personal data. For Phoenix STS Ltd., a company involved in fire, health, and safety management training, adhering to data protection laws and best practices is paramount.

Data Collection and Consent:

- ***Consent:*** We ensure that consent is obtained from delegates for the collection and use of their personal information.
- ***Minimisation:*** Collect only the necessary data for the training/service and nothing more.

Data Storage:

- ***Secure Storage Solutions:*** We use encrypted digital storage solutions to store delegate information. This includes secure, cloud-based services or encrypted hard drives.
- ***Access Control:*** We implement strict access controls so only authorised personnel can access the data.

Data Protection Compliance:

- ***GDPR Compliance:*** As a company operating under Irish and EU jurisdictions, we will comply with the General Data Protection Regulation (GDPR).
- ***Regular Audits:*** We conduct regular audits to ensure compliance with data protection laws and identify any potential vulnerabilities.

Data Encryption:
Encryption of Data: We encrypt sensitive data in transit (when sent over the internet) and at rest (when stored).

Physical Records:

- ***Secure Locking Systems:*** We use secure, locked filing systems where physical records are kept.
- ***Controlled Access:*** We limit access to physical records to authorised personnel only.

Data Retention and Disposal:

- ***Retention Policy:*** Our data retention policy specifies how long delegate information is kept and ensures it complies with legal requirements.
- ***Secure Disposal:*** When data is no longer needed, we ensure its secure and compliant disposal. For digital data, use data-wiping techniques. For physical records, use shredding or a similar destruction method.

Employee Training and Awareness:

- ***Regular Training:*** we provide training on data protection practices and the importance of confidentiality for all employees.
- ***Awareness of Phishing and Scams:*** We train staff to be aware of phishing attempts and other scams that could compromise data security.

Data Breach Response Plan:
Incident Response Plan: We have a clear response plan in case of a data breach, including steps to mitigate the breach, notification procedures, and strategies to prevent future incidents.

Review and Update Security Measures:
Continuous Improvement: We regularly review and update security measures to keep up with evolving threats and technological advancements.

Transparency and Communication:
Privacy Policy: We maintain a clear privacy policy detailing how delegate data is collected, used, stored, and protected, and we make it easily accessible to delegates.