Technical and organizational measures according to Article 32 GDPR

Insendi recognises that it acts in the role of Data Processor in relation to the provision of learning platform services to Clients under the auspices of the General Data Protection Regulations (GDPR). Insendi's services are designed such that Clients act in the role of Data Controller. Insendi is committed to meeting the requirements of GDPR as Data Processor and works with clients in their role as Data Controllers to keep personal data safe.

Insendi's learning platform is hosted using Amazon Web Services (AWS). AWS itself is fully compliant with the GDPR regulations, more details of which can be found here: AWS GDPR center.

Data Protection Definitions:

- **Data Controller -** A data controller is an organisation that had full authority to decide how and why personal data is to be processed, and that has the overall responsibility for the data. Insendi considers that the Client Universities are the Data Controllers for the data that is input into the Insendi platform.

- **Data Processor -** A data processor is an organisation that processes personal data on behalf of another organisation. Insendi considers itself as acting as the data processor on behalf of its clients using the platform.

1.0 Confidentiality

1.1 Access control

- Insendi ensures that devices used with the business are stored in a secure location and administers a policy of overnight storage.

1.2 Access control to systems

- Insendi has designed the platform so that access is gained by two factor authentication (2FA). All Insendi users will access the system via 2FA. Clients will access the platform via their own single sign on (SSO) system and as the Data Controller retains the responsibility for secure access by all their platform users through their own designated SSO system.

1.3 Access control of data

- Insendi will ensure logging of user access and role are timestamped. These logging records will be kept and archived for a period of 2 years.

1.4 Segregation control

- Access to the Learning Platform is provided by Insendi as a SAS service. All production data is held on one Database. Insendi has separate Databases for User Acceptance Tests, Development, QA, and Production. Insendi maintains separation is via the software on the production Database.

1.5 Pseudonymization

- Insendi will ensure that processing of personal data in a way that the data can no longer be assigned to a specific data subject without additional information being provided, if such additional information are kept separately and are subject to appropriate technical and organisational measures.

2.0 Integrity

2.1 Transfer control

- Data at rest is always encrypted. Insendi uses the following data standard SHA-256 with RSA Encryption. Data in transit is always via secure encrypted connections. The platform will facilitate the exporting of data for use by the Client. Once the data is exported the Client as Data Controller retains responsibility for is security.

2.2 Input control

- The Insendi Platform is designed to ensure that all personal data is tagged with a system wide unique ID. This is to facilitate logging and removal of data as required.

3.0 Availability

3.1 Availability control

- The system is regularly checked for proper functioning.
- The usage of the systems is monitored and an alarm is triggered in the event of a fault.
- Suitable measures are taken to prevent unauthorized intrusion into computers from the outside (virus protection / firewall).
- Insendi's platform availability measures are detailed within the Insendi backup policy which is available here; Backup Policy.

3.2 Quick recoverability

- Insendi platform recovery is detailed through the Insendi backup policy which is available here; Backup Policy.
- The Insendi development team will take prompt measures to restore data in the event of an emergency in the event of a physical or technical incident. Please ask your account representative about our Business Continuity and Disaster Recovery Plan.

4.0 Procedures for periodic review and evaluation

4.1 Data protection management

- Employees who process personal data are bound to data secrecy upon entering the company as part of our Insendi contract.
- Regulations on data protection are written down in various company guidelines (policies and guidelines).
- There is a process to guarantee the rights of data subjects to information, deletion, restriction of processing, data portability and correction of data.
- The responsibilities for equipment and systems have been defined.

4.2 Incident management

- There is a process for dealing with data protection incidents to ensure the fulfilment of reporting obligations to the supervisory authority and the data subjects. We will enable detection services on AWS with email alerts to notify Insendi if anything is triggered. We will always endeavour, within 24 hours of becoming aware of any incident, to inform you of the following:
  - What happened and how it happened.
  - What we have done to remedy the incident.
  - What are doing and plan to do to remedy the incident.
  - Who you can contact at Insendi to get more information and stay current with the situation.

4.3 Data protection friendly default setting according to Article 25 (2) GDPR

- Insendi signs up to the principle of data privacy by design and default through the organizational and technical arrangements set out within this policy. Further Insendi will review the state of the art on data security techniques and will bring forward suggested amendments to this policy on an annual review.

4.4 Order control

- Employees who e.g. enter, change or use personal data in data processing systems are obliged to maintain data secrecy upon entering the company.
- Regulations on data protection are written down in various company guidelines (policies and guidelines).