Appendix A – Technical and Organisational Measures

This appendix forms part of the Data Processing Agreement between EdBox AS and the educational institution using Whisperate.

EdBox AS implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with GDPR Article 32.

1. Access Control

- Role-based access control limiting access to personal data to authorised personnel only
- Principle of least privilege applied to all system access
- Multi-factor authentication for administrative access where applicable

2. Data Security

- Encryption of data in transit using industry-standard protocols
- Encryption of stored data where appropriate
- Secure key management practices

3. Hosting and Infrastructure

- Production data is hosted within the EU/EEA
- Primary hosting and database infrastructure provided by Supabase (Stockholm region)
- Underlying cloud infrastructure provided by Amazon Web Services (AWS)

4. Logging and Monitoring

- Logging of administrative access to systems processing personal data
- Logs are used for security monitoring and incident investigation
- Monitoring of system logs for security-relevant events where applicable

5. Backup and Recovery

- Encrypted daily backups of production data
- Retention of deleted data in encrypted backups for up to 7 days
- Procedures for secure restoration of data in case of system errors or data loss

6. Organisational Measures

- Confidentiality obligations for all personnel with access to personal data
- Internal policies governing data protection and information security
- Regular review of security practices

7. Incident Management

- Procedures for identifying, managing, and responding to security incidents

- Notification of the Data Controller without undue delay in the event of a personal data breach. Where EdBox AS does not have direct institutional contact details, notification shall be provided via the lecturers or administrators registered in Whisperate, acting as representatives of the Customer

8. Sub-processor Management

- Due diligence performed on sub-processors prior to engagement
- Contractual requirements ensuring compliance with applicable data protection legislation

9. Review and Updates

- These measures are reviewed periodically and updated where necessary to maintain an appropriate level of security