Schedule 6: Data Processing Agreement (DPA)

This Data Processing Agreement (**DPA**) forms part of the Licence Agreement between:

LearnWise Software International BV (**Processor** or **LearnWise**), with registered office at Kraanspoor 50, 1033 SE Amsterdam, Netherlands, and

The Customer as identified in the applicable Order (**Controller**)

Each a **Party** and together the **Parties**

1. SCOPE AND PRECEDENCE

1.1 This DPA applies to the Processing of Personal Data by LearnWise on behalf of the Customer in the course of providing the Services.

1.2 Unless otherwise defined in this DPA, capitalised terms have the meanings given in the Licence Agreement.

2. DEFINITIONS

2.1 **Customer Data** means Proprietary Information of the Customer and includes non-public data provided by the Customer to LearnWise to enable the provision of the Services.

2.2 **Files** means any information, including Customer Data, commercial data, technical information, and usage data.

2.3 **GDPR** means both (i) the General Data Protection Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the **UK GDPR**), and (ii) the General Data Protection Regulation (EU) 2016/679 (the **EU GDPR**), as applicable to the processing activities under the Licence Agreement.

2.4 **Personal Data** has the meaning given in Article 4 of the GDPR.

2.5 **Processing** has the meaning given in Article 4 of the GDPR.

2.6 **Proprietary Information** means any business, technical or financial information relating to a Party. Proprietary Information of LearnWise includes non-public information regarding the Service's features, functionality and performance. Proprietary Information of the Customer includes the Customer Data.

2.7 Other definitions align with Section 1 of the Licence Agreement.

3. PROCESSING OF PERSONAL DATA

3.1 Regional Processing

- All data processing occurs in the Controller's primary region (EU, UK, or US)
- EU customer data is processed in AWS Dublin
- UK customer data is processed in AWS London
- US customer data is processed in US AWS regions
- For customers with users in multiple regions, data is processed in the customer's primary business region

3.2 Processing Authority

- LearnWise processes Personal Data solely on documented instructions from the Controller
- Processing is limited to the scope necessary for Service provision as defined in the Licence Agreement
- No processing for LearnWise's own purposes except as follows:
    - LearnWise shall have the right collect and analyse data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, information concerning Customer Data and data derived therefrom), and LearnWise will be free (during and after the term hereof) to (i) use such information and data to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other LearnWise offerings, and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business

3.3 AI Processing

- LearnWise uses enterprise-grade AI providers (such as OpenAI and Anthropic) through secure AWS or Azure endpoints
- All AI processing remains within the customer's designated region
- No training of AI models occurs on customer data
- AI processing follows confidentiality requirements outlined in Section 4.2 of this DPA

3.4 Compliance with Instructions

- LearnWise shall immediately inform the Controller if, in its opinion, an instruction from the Controller infringes the GDPR or other applicable Union or Member State data protection provisions.

3.5 Compliance with Data Protection Laws

- LearnWise shall comply with all applicable data protection laws, including but not limited to the GDPR, in its processing of Personal Data under this DPA. LearnWise shall implement and maintain appropriate technical and organisational measures to ensure compliance with these laws and shall reasonably assist the Controller in fulfilling its obligations, including responding to data subject rights requests and conducting Data Protection Impact Assessments, insofar as this is possible taking into account the nature of the processing and the information available to LearnWise.

4. SECURITY AND CONFIDENTIALITY

4.1 Security Measures

- Compliance with security provisions in the Licence Agreement
- Regular security assessments and monitoring
- Access controls as specified in Annex B

4.2 Confidentiality

- Each Party (the **Receiving Party**) understands that the other party (the **Disclosing Party**) has disclosed or may disclose Proprietary Information relating to the Disclosing Party’s business. The Receiving Party agrees:
    - to take reasonable precautions to protect such Proprietary Information, and

    - not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information

- The Disclosing Party agrees that the foregoing shall not apply with respect to any information after five (5) years following the disclosure thereof or any information that the Receiving Party can document:

    - is or becomes generally available to the public, or

    - was in its possession or known by it prior to receipt from the Disclosing Party, or

    - was rightfully disclosed to it without restriction by a third party, or

    - was independently developed without the use of any Proprietary Information of the Disclosing Party or

    - is required to be disclosed by law

- All personnel bound by written confidentiality agreements

- Sub-processors subject to equivalent obligations

5. SUB-PROCESSORS

5.1 Appointment

- Current sub-processor list maintained at http://trust.learnwise.ai/

- 30-day advance notice of changes via trust@learnwise.ai

- Right to object to new sub-processors within 30 days

5.2 Sub-processor Obligations

- Written agreements including data protection obligations

- Regular monitoring and compliance verification

- LearnWise remains fully liable for sub-processor compliance

6. DATA SUBJECT RIGHTS

6.1 Support Obligations

- LearnWise assists Controller with data subject requests

- If the Customer provides Files to the Service or via other types of electronic communications to LearnWise, the Customer approves LearnWise's processing of the Files

- LearnWise guarantees that all Files will be used only for data processing purposes by the Service, and any third party will not have any access to the Customer's Files without the Customer's additional permission

- Technical tools provided for data access and deletion

6.2 Direct Requests

- Data subjects directed to Controller

- No direct response without Controller approval

7. PERSONAL DATA BREACHES

7.1 Notification

- Within 24 hours of breach detection, relating to data breaches
- Notification to designated security contact
- Details of impact and mitigation measures

7.2 Response

- Immediate containment measures
- Investigation and root cause analysis
- Regular status updates to Controller

8. AUDITS AND COMPLIANCE

8.1 Audit Rights

- Annual audit right with 30 days notice
- Access to security documentation
- Cooperation with regulatory authorities

8.2 Certifications

- LearnWise is certified and aligned with the SOC 2 and ISO 27001 frameworks. Reports and certifications are available at http://trust.learnwise.ai/
- Regular compliance updates
- Third-party audit reports available upon request

9. TERM AND TERMINATION

9.1 Duration

- Coterminous with the Licence Agreement
- Subject to termination provisions in Section 9 of the Licence Agreement

9.2 Data Return/Deletion

- 90-day retention period after Licence Agreement termination
- Data returned or deleted per Controller's choice
- Deletion certificate available upon request

10. LIABILITY AND INDEMNIFICATION

10.1 Liability provisions align with Section 8 of the Licence Agreement, except where mandatory data protection laws require otherwise.

10.2 Indemnification obligations follow Section 7 of the Licence Agreement.

11. GOVERNING LAW

11.1 This DPA is governed by English law and subject to the exclusive jurisdiction of the English courts, in accordance with the governing law provisions of the Licence Agreement.

ANNEX A: PROCESSING DETAILS

1. Categories of Data Subjects

- Students using the LearnWise platform
- Faculty and staff members
- Administrators and support staff
- Website visitors (if applicable)
- Other authorised users granted access by the Controller

2. Categories of Personal Data

2.1 Basic User Data

- Names (first and last)
- Email addresses
- User roles and permissions
- Institutional affiliations
- Authentication credentials

2.2 Educational Data

- Course enrolments
- Assignment data
- Support queries
- Learning interactions
- Course content interactions

2.3 Technical Data

- IP addresses
- Browser information
- Device details
- Session data
- Usage analytics

2.4 Integration-Specific Data

2.4.1 LMS Integration Data

- Course structure data
- Enrolment information

- Assignment details
- Educational resources
- User progress data

2.4.2 API Integration Data

- Authentication tokens
- API call logs
- Integration metadata
- System identifiers

2.4.3 SSO Integration Data

- Authentication tokens
- User profile data
- Session information

3. Processing Operations

3.1 Core Processing Activities

- User authentication and authorization
- Service delivery and personalization
- AI-powered educational support
- Analytics and reporting
- Technical support

3.2 AI Processing Specifications

- Processing through enterprise AI providers
- Regional data processing enforcement
- No AI model training on customer data
- Usage pattern analysis for service improvement

ANNEX B: SECURITY MEASURES

1. Access Control

1.1 Physical Access Control

- AWS data centre security controls
- Restricted physical access to servers
- Environmental protection measures
- 24/7 monitoring

1.2 System Access Control

- Multi-factor authentication (MFA)
- Role-based access control (RBAC)
- Regular access reviews
- Automatic session termination
- Password policy enforcement

1.3 Data Access Control

- Least privilege principle
- Data segregation by customer
- Access logging and monitoring
- Regular permission audits

2. Transmission Control

2.1 Encryption Standards

- TLS 1.2/1.3 for data in transit
- AES-256 for data at rest
- Secure key management through AWS KMS
- Certificate management

2.2 Network Security

- Network segregation
- Firewall protection
- Regular penetration testing
- Intrusion detection/prevention

3. Input Control

- Activity logging
- Audit trail maintenance
- Change management procedures
- Access attempt monitoring

4. Availability Control

- Regular backups
- Disaster recovery procedures
- Business continuity planning
- Redundant systems

5. Separation Control

- Customer data segregation
- Development/production separation
- Testing environment isolation
- Data processing separation

ANNEX C: SUB-PROCESSOR MANAGEMENT

1. Current Critical Sub-processors

1.1 Infrastructure Providers

- Amazon Web Services (AWS)
- Purpose: Hosting and infrastructure
- Location: Regional data centres (EU/UK/US)
- Security certifications: Available at http://trust.learnwise.ai/compliance

1.2 AI Processing Providers

- Enterprise AI providers (e.g., OpenAI, Anthropic)
- Purpose: AI processing through secure endpoints
- Location: Matches customer's region through AWS/Azure
- Security controls: Enterprise API integration only

1.3 Monitoring and Security

- Security monitoring providers
- Analytics services
- Performance monitoring Complete list maintained at http://trust.learnwise.ai/

2. Sub-processor Requirements

2.1 Minimum Security Standards

- ISO 27001/SOC 2 certification
- GDPR compliance
- Regular security assessments
- Incident response capabilities

2.2 Contractual Requirements

- Data processing agreements
- Confidentiality obligations
- Security requirements
- Audit rights

2.3 Monitoring and Compliance

- Annual security reviews
- Performance monitoring

- Compliance verification
- Regular audits

3. Change Management

3.1 Notification Process

- 30-day advance notice
- Impact assessment
- Security evaluation
- Customer objection rights

3.2 Documentation Requirements

- Security documentation
- Compliance certificates
- Processing records
- Audit reports

ANNEX D: BREACH NOTIFICATION PROCEDURES

1. Incident Response Timeline

- 0-24 hours: Initial detection and notification
- 24-48 hours: Impact assessment and updates
- 48-72 hours: Mitigation measures
- 72+ hours: Regular status updates

2. Required Notification Information

- Incident description
- Data types affected
- Impact assessment
- Mitigation measures
- Ongoing updates

3. Communication Channels

- Primary: trust@learnwise.ai
- Secondary: Designated technical contact
- Emergency: Security hotline (provided to customers at request)

4. Documentation Requirements

- Incident logs
- Investigation reports
- Mitigation records
- Communication records

If you have any questions in regards to this DPA or terms, please contact us at trust@learnwise.ai.