DATA PROCESSING AGREEMENT

Version: 2025.1

Document Reference: DPA-UNIHELPER-2025

Last Updated: [DATE]

ISO 27001 Aligned

PREAMBLE

This Data Processing Agreement (hereinafter referred to as the "**DPA**" or "**Agreement**") is entered into as of __________ (the "**DPA Effective Date**") and forms an integral and inseparable part of the Software Access Agreement, License Agreement, Terms of Service, or other written or electronic agreement (the "**Principal Agreement**") for the provision of services between:

THE DATA CONTROLLER:

Institution/Organization Name: ________________________________

Legal Form: ________________________________

Registration Number: ________________________________

VAT/Tax ID: ________________________________

Registered Address: ________________________________

Country of Establishment: ________________________________

Representative Name: ________________________________

Representative Title: ________________________________

Representative Email: ________________________________

Data Protection Officer (if appointed): ________________________________

(hereinafter referred to as the "**Controller**", "**Customer**", "**Institution**", or "**Educational Institution**")

THE DATA PROCESSOR:

Company Name: UniHelper ApS

Legal Form: Anpartsselskab (Private Limited Company)

Company Registration Number: CVR 39750007

VAT Number: DK39750007

Registered Office: Slotsgade 17B, 6200 Aabenraa, Denmark
Country of Establishment: Denmark
Representative: [Name of Authorized Signatory]
Title: [Title]
Data Protection Officer: Available at contact@unihelper.io

(hereinafter referred to as the "**Processor**", "**UniHelper**", "**Service Provider**", or "**Company**")
The Controller and Processor may be referred to individually as a "**Party**" and collectively as the "**Parties**".

RECITALS

WHEREAS, the Controller has determined that it requires specialized software services for the optimization and automation of student group formation within its educational programs, and has selected the Processor based on its expertise, technical capabilities, and commitment to data protection;

WHEREAS, the Processor has developed and operates a proprietary cloud-based software-as-a-service platform known as the UniHelper system (the "**Services**" or "**Platform**"), which utilizes advanced algorithms and data processing techniques to facilitate optimal group composition based on multiple compatibility factors;

WHEREAS, the performance of the Services necessarily requires the Processor to undertake certain processing operations on personal data relating to students, faculty, and administrative personnel of the Controller, such processing being integral to the delivery of the contracted Services;

WHEREAS, the Parties acknowledge that such processing of personal data must be conducted in strict compliance with applicable data protection legislation, including but not limited to:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation or "**GDPR**")
- Directive (EU) 2016/680 (Law Enforcement Directive)
- Regulation (EU) 2018/1807 (Free Flow of Non-Personal Data)
- National implementing legislation in EU Member States
- The UK General Data Protection Regulation and Data Protection Act 2018

- Applicable international data protection frameworks and standards

WHEREAS, the Parties recognize their respective obligations under Article 28 of the GDPR and equivalent provisions in other applicable data protection laws, which require that processing by a processor be governed by a contract that is binding on the processor with regard to the controller;

WHEREAS, the Parties wish to set forth their rights, responsibilities, and obligations with respect to the processing of personal data in a manner that ensures compliance with all applicable legal requirements while facilitating the effective delivery of the Services;

WHEREAS, the Parties acknowledge the fundamental rights and freedoms of data subjects and commit to implementing appropriate technical and organizational measures to ensure the protection of personal data;

NOW, THEREFORE, in consideration of the mutual covenants, terms, conditions, and agreements contained herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

ARTICLE 1: DEFINITIONS AND INTERPRETATION

1.1 Definitions

For the purposes of this Agreement, the following terms shall have the meanings ascribed to them below:

1.1.1 **"Applicable Data Protection Law"** means all laws, regulations, regulatory requirements, regulatory guidance, codes of practice, and industry standards applicable to the processing of personal data under this Agreement, including without limitation:

- The GDPR and any successor EU legislation
- EU Member State laws supplementing or implementing the GDPR
- The UK GDPR and UK Data Protection Act 2018
- The Federal Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, where applicable
- The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506, where applicable
- The California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA)
- Other U.S. state privacy laws including but not limited to those of Colorado, Connecticut, Utah, and Virginia
- Sector-specific regulations applicable to educational institutions
- Any binding decisions, opinions, or guidance issued by competent supervisory authorities

1.1.2 **"Personal Data"** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.1.3 **"Special Categories of Personal Data"** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

1.1.4 **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.1.5 **"Data Subject"** means the identified or identifiable natural person to whom the Personal Data relates, including but not limited to students, prospective students, alumni, faculty members, administrative staff, and other individuals whose Personal Data is processed under this Agreement.

1.1.6 **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, regardless of whether such breach results in risk to the rights and freedoms of natural persons.

1.1.7 **"Sub-processor"** means any natural or legal person, public authority, agency, or other body engaged by the Processor or its affiliates to process Personal Data on behalf of the Controller in connection with this Agreement. Sub-processors are included in **Annex II**.

1.1.8 **"Supervisory Authority"** means an independent public authority established by an EU Member State pursuant to Article 51 of the GDPR or equivalent authority in other jurisdictions.

1.1.9 **"Standard Contractual Clauses"** or **"SCCs"** means the standard contractual clauses for the transfer of personal data to processors established in third countries as adopted by the European Commission or equivalent mechanisms.

1.1.10 **"Services"** means the UniHelper cloud-based software-as-a-service platform for student group optimization and collaboration, including all associated features, functionalities, algorithms, interfaces, and technical infrastructure as more particularly described in the Principal Agreement and its annexes.

1.1.11 **"Data Protection Impact Assessment"** or **"DPIA"** means an assessment of the impact of envisaged processing operations on the protection of personal data as required under Article 35 of the GDPR.

1.1.12 **"Technical and Organizational Measures"** or **"TOMs"** means the measures aimed at protecting Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

1.2 Interpretation

1.2.1 References to statutory provisions shall be construed as references to those provisions as amended, consolidated, re-enacted, or replaced from time to time.

1.2.2 Headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement.

1.2.3 Words importing the singular include the plural and vice versa.

1.2.4 Any reference to "including" or "includes" means "including without limitation" or "includes without limitation."

1.2.5 Terms defined in the GDPR but not explicitly defined herein shall have the meanings given to them in the GDPR.

ARTICLE 2: RELATIONSHIP AND ROLES OF THE PARTIES

2.1 Designation of Roles

2.1.1 The Parties expressly acknowledge and agree that with respect to the Processing of Personal Data pursuant to this Agreement:

- The Customer acts as the Data Controller, determining the purposes and means of the Processing
- UniHelper acts as the Data Processor, processing Personal Data solely on behalf of and under the instructions of the Controller

2.1.2 This designation of roles reflects the factual allocation of responsibilities between the Parties and is binding for all purposes under Applicable Data Protection Law.

2.2 Purpose Limitation

2.2.1 The Processor acknowledges that it has no rights to process Personal Data for any purpose other than:

- The provision of the Services as specified in the Principal Agreement
- Compliance with the documented instructions of the Controller
- Compliance with legal obligations to which the Processor is directly subject

2.2.2 The Processor shall not process Personal Data for its own commercial purposes, including but not limited to marketing, product development (except as anonymized data), or sale to third parties.

2.3 Controller's Regulatory Compliance

2.3.1 The Controller represents and warrants that:

- It has all necessary rights, permissions, and lawful bases to provide Personal Data to the Processor
- Its instructions comply with Applicable Data Protection Law
- It has provided or will provide all necessary privacy notices to Data Subjects
- It has obtained or will obtain all necessary consents where required
- It has conducted or will conduct any required DPIAs

2.3.2 The Controller acknowledges sole responsibility for:

- The accuracy, integrity, and legality of Personal Data
- The means by which the Personal Data was acquired
- Determining the legal basis for Processing
- Responding to Data Subject requests (with Processor assistance as specified herein)

2.4 Independence of the Parties

2.4.1 Nothing in this Agreement shall be construed as creating a partnership, joint venture, agency, or employment relationship between the Parties.

2.4.2 Neither Party shall have authority to bind the other Party except as expressly provided in this Agreement.

ARTICLE 3: SCOPE AND DETAILS OF PROCESSING

3.1 Subject Matter of Processing

The subject matter of the Processing under this Agreement consists of the processing operations necessary for the Processor to provide the Services, specifically:

- Implementation and operation of the group formation platform
- Collection and analysis of student preference, availability, demographic, skills, and other relevant group formation data the educational institution requests, and in accordance with the educational institution's privacy policies.
- Algorithmic optimization of group compositions
- Facilitation of communication regarding group assignments
- Evaluate group working process and performance from a student perspective and collect student peer evaluations and feedback
- Generation of analytics and reports (in anonymized form)
- Technical support and system maintenance

3.2 Duration of Processing

3.2.1 **Commencement**: Processing shall commence upon the later of:

- The DPA Effective Date
- The first upload or transmission of Personal Data to the Services
- The activation of Customer's account on the Platform

3.2.2 **Active Processing Period**: Processing shall continue throughout the term of the Principal Agreement, including any renewal periods.

3.2.3 **Post-Termination Processing**: Limited processing may continue after termination solely for:

- Data return or deletion obligations (maximum 30 days)
- Compliance with legal retention requirements
- Defense of legal claims

3.3 Nature and Purpose of Processing

3.3.1 **Nature of Processing Operations**:

- **Collection**: Via secure web questionnaires and API integrations
- **Recording**: In cloud-based databases with encryption
- **Organization**: According to institutional structures and courses
- **Structuring**: For algorithmic analysis and optimization
- **Storage**: In EU-based data centers (primary) with secure backups, and in the US (sub-processing via Typeform) with AWS' GDPR compliant services
- **Retrieval**: Through authenticated access portals
- **Consultation**: For support and quality assurance purposes

- **Use**: For group formation algorithms and service delivery
- **Disclosure**: Only to authorized users within the Controller's organization
- **Deletion**: According to retention schedules and instructions

3.3.2 **Purposes of Processing**: The sole purposes are to enable the Controller to:

- Automate and optimize student group formation
- Improve educational outcomes through compatible group composition
- Reduce administrative burden on faculty and staff
- Provide data-driven insights into group dynamics
- Facilitate communication among group members

3.4 Categories of Personal Data

Details of Personal Data categories are set forth in **Annex I**, which forms an integral part of this Agreement.

3.5 Categories of Data Subjects

Details of Data Subject categories are set forth in **Annex I**, which forms an integral part of this Agreement.

ARTICLE 4: PROCESSOR'S OBLIGATIONS

4.1 Processing According to Instructions

4.1.1 The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by applicable law to which the Processor is subject, in which case the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.1.2 The Processor confirms that the Controller's instructions as set out in this Agreement, including its Annexes, constitute the complete and final documented instructions. Any additional or alternate instructions must be agreed upon in writing.

4.1.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection provisions. The Processor shall be entitled to suspend execution of the relevant instruction until the Controller confirms or modifies it.

4.1.4 The Processor shall maintain comprehensive records of all processing activities carried out on behalf of the Controller, containing at minimum the information required under Article 30 of the GDPR.

4.2 Confidentiality

4.2.1 The Processor shall ensure that all persons authorized to process Personal Data:

- Have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Receive appropriate training on data protection requirements
- Are aware of the sensitive nature of Personal Data
- Understand the consequences of unauthorized disclosure

4.2.2 The confidentiality obligations shall survive termination of this Agreement indefinitely or for the maximum period permitted by applicable law.

4.2.3 The Processor shall implement and maintain policies and procedures to ensure ongoing compliance with confidentiality requirements, including but not limited to:

- Confidentiality agreements with all employees and contractors
- Regular training and awareness programs
- Disciplinary measures for breaches of confidentiality
- Access controls and monitoring systems

4.3 Security of Processing

4.3.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

4.3.2 The specific technical and organizational measures implemented by the Processor are detailed in **Annex II**. The Processor shall maintain and update these measures as necessary to address evolving threats and vulnerabilities.

4.3.3 The Processor shall regularly test, assess, and evaluate the effectiveness of technical and organizational measures for ensuring the security of the processing, including but not limited to:

- Annual penetration testing
- Quarterly vulnerability assessments
- Continuous security monitoring
- Security reviews (quarterly, annual)

4.4 Use of Sub-processors

4.4.1 **General Authorization with Right to Object**: The Controller hereby provides general authorization for the Processor to engage Sub-processors listed in **Annex III**, subject to the following conditions:

- The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors
- Such notification shall be provided at least thirty (30) calendar days in advance
- The Controller may object to such changes on reasonable grounds relating to data protection
- If the Parties cannot resolve the objection, either Party may terminate the affected Services

4.4.2 **Sub-processor Obligations**: The Processor shall:

- Enter into written agreements with Sub-processors imposing data protection obligations no less protective than those in this Agreement
- Remain fully liable for any Sub-processor's acts or omissions
- Conduct due diligence on all Sub-processors before engagement
- Monitor Sub-processor compliance through regular audits and assessments
- Ensure Sub-processors implement appropriate technical and organizational measures

4.4.3 **Information Requirements**: For each Sub-processor, the Processor shall maintain and provide:

- Full legal name and registration details

- Contact information including data protection contacts
- Description of processing activities performed
- Locations of processing and data storage
- Applicable safeguards for international transfers
- Copies of data processing agreements upon reasonable request

4.5 International Data Transfers

4.5.1 The Processor shall not transfer Personal Data outside the European Economic Area ("EEA") without:

- Prior written authorization from the Controller
- Implementation of appropriate safeguards under Chapter V of the GDPR
- Compliance with any supplementary measures required following the Schrems II judgment

4.5.2 Where transfers are authorized, the Processor shall:

- Execute Standard Contractual Clauses or rely on other valid transfer mechanisms
- Conduct transfer impact assessments
- Implement supplementary technical measures where necessary
- Maintain documentation of all transfers and safeguards
- Notify the Controller of any developments affecting transfer legality

4.6 Data Subject Rights

4.6.1 The Processor shall, insofar as possible taking into account the nature of the processing, assist the Controller by implementing appropriate technical and organizational measures for the fulfillment of the Controller's obligations to respond to requests for exercising Data Subject rights under Chapter III of the GDPR.

4.6.2 The Processor shall:

- Forward any Data Subject request received directly to the Controller without undue delay
- Not respond to Data Subjects directly unless authorized by the Controller
- Maintain capabilities to support all Data Subject rights including:
    - Right of access (Article 15 GDPR)
    - Right to rectification (Article 16 GDPR)
    - Right to erasure/right to be forgotten (Article 17 GDPR)
    - Right to restriction of processing (Article 18 GDPR)
    - Right to data portability (Article 20 GDPR)
    - Right to object (Article 21 GDPR)
    - Rights related to automated decision-making (Article 22 GDPR)

4.6.3 Detailed procedures for assisting with Data Subject rights are set forth in **Annex IV**.

4.7 Personal Data Breach Management

4.7.1 The Processor shall notify the Controller without undue delay and in any event within twenty-four (24) hours after becoming aware of a Personal Data Breach affecting Personal Data processed under this Agreement.

4.7.2 Such notification shall include, at minimum:

- Nature of the Personal Data Breach including categories and approximate numbers of Data Subjects and Personal Data records concerned
- Name and contact details of the data protection officer or other contact point
- Likely consequences of the Personal Data Breach
- Measures taken or proposed to address the breach and mitigate its possible adverse effects

4.7.3 The Processor shall:

- Cooperate fully with the Controller in investigating and remediating the breach
- Document all breaches regardless of risk level
- Implement measures to prevent recurrence
- Provide regular updates on breach resolution
- Preserve evidence for potential regulatory investigations

4.8 Data Protection Impact Assessments and Prior Consultation

4.8.1 The Processor shall provide reasonable assistance to the Controller with:

- Data protection impact assessments under Article 35 GDPR
- Prior consultation with supervisory authorities under Article 36 GDPR

4.8.2 Such assistance may include:

- Providing information about technical and organizational measures
- Participating in risk assessments
- Suggesting mitigation measures
- Reviewing DPIA documentation

4.9 Deletion and Return of Personal Data

4.9.1 Upon termination of the Services or upon the Controller's written request, the Processor shall, at the choice of the Controller:

- Delete all Personal Data and existing copies within thirty (30) days
- Return all Personal Data in a structured, commonly used, and machine-readable format

4.9.2 The Processor shall:

- Provide written certification of deletion signed by an authorized representative
- Ensure deletion from all systems including backups (where technically feasible)
- Retain Personal Data only to the extent required by applicable law
- Ensure Sub-processors also delete or return Personal Data

4.10 Audit and Compliance

4.10.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

4.10.2 The Processor shall:

- Respond to reasonable audit questionnaires within thirty (30) days
- Provide, if available, third-party audit reports (e.g., ISAE 3000, SOC 2)
- Permit remote, document only, audits with sixty (60) days advance notice
- Bear its own costs for standard audits (Controller bears costs for additional audits)

4.10.3 The Processor may object to an auditor if:

- The auditor is a competitor of the Processor
- The auditor is not bound by confidentiality obligations
- The audit would violate applicable law or professional standards

ARTICLE 5: CONTROLLER'S OBLIGATIONS

5.1 Lawfulness of Processing

The Controller represents, warrants, and undertakes that:

5.1.1 It has established and will maintain appropriate legal bases for all Processing under Article 6 GDPR (and Article 9 where applicable).

5.1.2 All instructions issued to the Processor comply with Applicable Data Protection Law.

5.1.3 It has fulfilled and will continue to fulfill all transparency obligations under Articles 13 and 14 GDPR.

5.1.4 Where consent is relied upon as a legal basis:

- Such consent meets all requirements of Articles 4(11) and 7 GDPR
- Appropriate mechanisms exist to record and manage consent
- Procedures are in place to honor consent withdrawal

5.2 Data Quality and Accuracy

The Controller shall ensure that:

5.2.1 All Personal Data provided is accurate, current, and complete.

5.2.2 Personal Data is adequate, relevant, and limited to what is necessary for the purposes (data minimization).

5.2.3 Appropriate processes exist to maintain data accuracy throughout the processing lifecycle.

5.2.4 No Special Categories of Personal Data are provided unless specifically agreed in writing.

5.3 Cooperation and Information

The Controller shall:

5.3.1 Provide timely responses to Processor requests for clarification or guidance.

5.3.2 Maintain current contact information for all compliance-related communications.

5.3.3 Promptly notify the Processor of any changes affecting processing obligations.

5.3.4 Cooperate in good faith to resolve any data protection issues that arise.

ARTICLE 6: LIABILITY AND INDEMNIFICATION

6.1 Statutory Liability

6.1.1 Each Party's liability for damages under the GDPR shall be determined in accordance with Article 82 GDPR.

6.1.2 The Processor shall be liable for damages caused by processing only where it has:

- Not complied with obligations of the GDPR specifically directed to processors
- Acted outside or contrary to lawful instructions of the Controller

6.2 Contractual Liability

6.2.1 Subject to Section 6.1, each Party's total aggregate liability arising out of or related to this Agreement shall be subject to the limitations and exclusions set forth in the Principal Agreement.

6.2.2 Nothing in this Agreement shall limit either Party's liability for:

- Death or personal injury caused by negligence
- Fraud or fraudulent misrepresentation
- Any liability that cannot be excluded or limited under applicable law

6.3 Indemnification

6.3.1 **Controller Indemnification**: The Controller shall defend, indemnify, and hold harmless the Processor from and against all claims, damages, losses, and expenses (including reasonable attorneys' fees) arising from:

- The Controller's breach of Applicable Data Protection Law
- The Controller's breach of this Agreement
- Claims that the Controller lacked necessary rights or permissions for the Processing
- The Controller's unlawful instructions

6.3.2 **Processor Indemnification**: The Processor shall defend, indemnify, and hold harmless the Controller from and against all claims, damages, losses, and expenses (including reasonable attorneys' fees) arising from:

- The Processor's breach of this Agreement
- The Processor's processing outside or contrary to lawful instructions
- The Processor's breach of Applicable Data Protection Law specifically directed to processors

6.3.3 **Indemnification Procedures**:

- The indemnified Party shall promptly notify the indemnifying Party of any claim
- The indemnifying Party shall have the right to control the defense
- The indemnified Party shall provide reasonable cooperation
- No settlement shall be made without the indemnified Party's consent (not to be unreasonably withheld)

ARTICLE 7: TERM AND TERMINATION

7.1 Term

This Agreement shall:

- Commence on the DPA Effective Date
- Continue for the duration of the Principal Agreement
- Automatically renew with any renewal of the Principal Agreement
- Terminate automatically upon termination of the Principal Agreement

7.2 Termination for Cause

Either Party may terminate this Agreement immediately upon written notice if:

- The other Party materially breaches this Agreement and fails to cure within thirty (30) days of written notice
- The other Party breaches Applicable Data Protection Law in a manner that cannot be cured
- Continued performance would violate Applicable Data Protection Law

7.3 Effects of Termination

Upon termination:

- The Processor shall cease all Processing except as required for compliance with legal obligations
- The provisions of Section 4.9 (Deletion and Return) shall apply
- All rights and licenses granted hereunder shall immediately terminate
- Provisions that by their nature should survive shall remain in effect

ARTICLE 8: GENERAL PROVISIONS

8.1 Governing Law and Jurisdiction

8.1.1 This Agreement shall be governed by and construed in accordance with the laws of Denmark, without regard to its conflict of law provisions.

8.1.2 Any dispute arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of Copenhagen, Denmark.

8.1.3 Notwithstanding the foregoing, either Party may seek injunctive or other equitable relief in any court of competent jurisdiction.

8.2 Amendment and Modification

8.2.1 This Agreement may only be amended or modified by written agreement executed by authorized representatives of both Parties.

8.2.2 The Processor may update Annexes to reflect:

- Changes in Sub-processors (subject to objection rights)
- Improvements to technical and organizational measures
- Updates required by changes in Applicable Data Protection Law

8.3 Severability

If any provision of this Agreement is held to be invalid, illegal, or unenforceable:

- The validity, legality, and enforceability of the remaining provisions shall not be affected

- The Parties shall negotiate in good faith to replace the invalid provision with a valid provision that achieves the original intent

8.4 Entire Agreement

8.4.1 This Agreement, including all Annexes, constitutes the entire agreement between the Parties with respect to the processing of Personal Data and supersedes all prior or contemporaneous agreements, understandings, and communications.

8.4.2 In the event of any conflict:

- Between this Agreement and the Principal Agreement regarding data protection matters, this Agreement shall prevail
- Between the body of this Agreement and the Annexes, the body shall prevail unless explicitly stated otherwise
- Between different language versions, the English version shall prevail

8.5 Notices

8.5.1 All notices under this Agreement shall be:

- In writing
- Delivered to the addresses specified in the preamble (or as subsequently updated)
- Sent via email with confirmation of receipt, registered mail, or internationally recognized courier

8.5.2 Notices shall be deemed received:

- Email: upon confirmation of receipt
- Registered mail: five (5) business days after posting
- Courier: upon signed receipt

8.6 Force Majeure

Neither Party shall be liable for any failure or delay in performance caused by circumstances beyond its reasonable control, including but not limited to acts of God, natural disasters, war, terrorism, riots, embargoes, acts of civil or military authorities, fire, floods, accidents, pandemics, strikes, or shortages of transportation, facilities, fuel, energy, labor, or materials.

8.7 Assignment

Neither Party may assign, transfer, or delegate any rights or obligations under this Agreement without the prior written consent of the other Party, except:

- The Processor may assign to an affiliate or in connection with a merger, acquisition, or sale of all or substantially all of its assets
- Upon assignment, the assignee shall assume all obligations under this Agreement

8.8 Third-Party Beneficiaries

This Agreement is intended solely for the benefit of the Parties and their permitted successors and assigns. Nothing in this Agreement confers any rights or remedies upon any third party.

8.9 Relationship of Parties

The Parties are independent contractors. Nothing in this Agreement creates any agency, partnership, joint venture, or employment relationship.

8.10 Waiver

No waiver of any provision of this Agreement shall be effective unless in writing and signed by the waiving Party. No waiver shall constitute a waiver of any other provision or a continuing waiver.

8.11 Counterparts

This Agreement may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument. Electronic signatures shall be deemed valid and binding.

ARTICLE 9: DEFINITIONS FOR U.S. EDUCATIONAL INSTITUTIONS

Where the Controller is a U.S. educational institution, the following additional definitions and modifications apply:

9.1 FERPA Definitions

9.1.1 **"Education Records"** has the meaning set forth in 20 U.S.C. § 1232g and 34 CFR Part 99.

9.1.2 **"School Official"** means a party to whom an educational institution has outsourced services or functions it would otherwise use employees to perform.

9.1.3 **"Legitimate Educational Interest"** means the need to review education records to fulfill professional responsibilities for the educational institution.

9.2 COPPA Definitions

9.2.1 **"Child"** means an individual under the age of 13.

9.2.2 **"Verifiable Parental Consent"** means consent that meets the requirements of 16 CFR § 312.5.

SIGNATURES

IN WITNESS WHEREOF, the Parties have executed this Data Processing Agreement as of the date last written below.

FOR THE DATA CONTROLLER:

Signature: ________________________________

Print Name: ______________________________

Title: ___________________________________

Date: ____________________________________

FOR THE DATA PROCESSOR:

Signature: ________________________________

Print Name: ______________________________

Title: ___________________________________

Date: ____________________________________

ANNEX I - DETAILS OF PROCESSING

1. SUBJECT MATTER OF PROCESSING

1.1 Detailed Description

The Processor shall undertake the following processing operations in the provision of the Services:

1.1.1 Data Collection and Intake

- Implementation and operation of secure web-based questionnaires
- API integration with Controller's learning management systems (where applicable)
- Microsoft Entra Single Sign-On (SSO) (for instructors)
- Secure file transfer protocol (SFTP) data imports
- Manual data entry interfaces for administrators
- Validation and verification of data upon collection

1.1.2 Data Processing and Analysis

- Algorithmic analysis using proprietary group optimization algorithms
- Compatibility scoring based on multiple weighted factors
- Availability matching and scheduling optimization
- Performance prediction modeling
- Statistical analysis for reporting purposes

1.1.3 Data Storage and Management

- Secure storage in encrypted cloud databases
- Redundant backup systems with geographic distribution
- Version control and audit trail maintenance
- Data lifecycle management according to retention policies
- Archive and retrieval systems

1.1.4 Data Distribution and Communication

- Secure delivery of group assignments to authorized users
- Email notification systems for students and administrators
- Export functionality

1.1.5 Access Control and User Management

- Authentication and authorization of users (students, instructors, administrators)
- Role-based access management and least-privilege enforcement
- Logging and monitoring of access attempts and session activity
- Automated session timeout and credential revocation processes

1.1.6 Data Pseudonymization, Anonymization, and Minimization

- Pseudonymization of personal data for analytics and reporting
- Anonymization or aggregation of data for research, benchmarking, and product improvement
- Data minimization practices ensuring only strictly necessary data is collected and processed
- Automated deletion of transient identifiers once processing is complete

1.1.7 Incident Detection and Security Monitoring

- Continuous monitoring of systems for unauthorized access or anomalous activity
- Logging, detection, and notification of personal data breaches in accordance with Article 33 GDPR
- Implementation of automated alerts and incident response workflows

1.1.8 Data Subject Rights Facilitation

- Support for data subject access, rectification, restriction, and erasure requests
- Export of personal data in structured, commonly used, machine-readable formats (Article 20 portability)
- Mechanisms for the Controller to review and approve responses before release

1.1.9 Sub-Processor Management

- Onboarding, due diligence, and continuous oversight of approved sub-processors
- Maintenance of an up-to-date sub-processor register
- Secure data transfer and contractual safeguards when engaging sub-processors outside the EEA

1.1.10 International Data Transfers (if applicable)

- Transfers outside the EEA performed under appropriate safeguards (e.g., EU SCCs, adequacy decisions)
- Maintenance of transfer impact assessments (TIAs) where required under Schrems II obligations

1.1.11 Testing, QA, and Development Environments

- Use of pseudonymized or synthetic data in non-production environments
- Strict separation of production and development environments
- Controlled access and logging for any processing in staging or QA systems

1.1.12 Deletion and Return of Data

- Secure erasure of data following contract termination or at the Controller’s written request
- Return of personal data to the Controller in agreed-upon format before deletion
- Cryptographic wipe procedures and certificate of deletion upon completion

ANNEX II - SUB-PROCESSORS

Company	Purpose	Location
Google	Business Network	EU
Amazon Web Services (AWS)	Cloud Hosting, Data Protection, Log Monitoring	EU
Zoho	Customer Relationship Management	EU
Proton Technologies	Customer Communications	Switzerland
Typeform	Hosting Questionnaires	US