PERSONAL DATA PROCESSING AGREEMENT

This Data Processing Agreement (henceforth, “DPA”) forms an integral part of the service agreement (henceforth, “the Service Agreement”) concluded between the customer (henceforth, “Customer”) and Alemira AG (henceforth, “Alemira”). Customer and Alemira are each a “Party” and, collectively, the “Parties”.

This DPA (and Standard Contractual Clauses as applicable according to Annex V) shall be considered pre-signed by Alemira.

By entering into the Service Agreement, Customer is deemed to have signed the DPA and the Standard Contractual Clauses in Annex V, as of the effective date of the Service Agreement.

Insofar as this DPA forms an integral part of the Service Agreement concluded between Customer and Alemira, it shall become effective on the Service Agreement’s effective date.

During the performance of its obligations according to the Service Agreement, Alemira may process Customer Personal Data. Insofar as Alemira is required to process Customer Personal Data pursuant to the Service Agreement, the Parties hereby agree that the terms of this DPA shall apply.

This DPA shall prevail over any other existing data processing agreement or similar arrangement between Alemira and the Customer that may already be in place.

1. DEFINED TERMS

In this DPA:

(a) Terms such as “Controller,” “Data Subject,” “Personal Data," “Processing”, “Data Breach”, and “Processor” shall have the meanings provided in Art. 4 GDPR.

“Applicable Data Protection Law” means all laws and regulations applicable to Customer and Alemira’s processing of personal data under the DPA.

“Customer Account Data” means personal data that relates to Customer’s relationship with Alemira, including the names or contact information of individuals authorized by Customer to access Customer’s account, and billing information of individuals that Customer has associated with its account. Customer Account Data also includes any personal data Alemira may need to collect for the purpose of identity verification or for the purpose of complying with its legal obligations.

“Customer Usage Data” means data processed by Alemira for the purposes of analyzing and evaluating Customer Content. Customer Usage Data includes data used to identify the source and destination of a communication, such as (a) the date, time, duration and the type of data exchange and (b) activity logs used to identify the source of Service requests, optimize and maintain performance of the Services, and investigate and prevent system abuse.

“Customer Content” means (a) personal data exchanged as a result of using the Service(s) such as message texts, voice and video media, images, email texts, email recipients, sound, and, where applicable, details Customer submits to the Service(s) from its designated software applications and

services and (b) data stored on Customer's behalf such as communication logs within the Service(s) or data that Customer has uploaded to the Service(s) (as defined in the Service Agreement).

"Customer Data" has the meaning given in the Service Agreement. Customer Data includes Customer Account Data, Customer Usage Data, Customer Content, and Sensitive Data, each as defined in this DPA.

"Special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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.

"Sub-processor" means (a) Alemira, when Alemira is processing Customer Content and where Customer is a processor of such Customer Content or (b) any third-party processor engaged by Alemira to process Customer Content in order to provide the Services to Customer.

"Third Party Request" means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

"Alemira Privacy Notice" means the privacy notice for the Services, the current version of which is available at https://www.constructor.tech/privacy-policy.

Any other capitalized terms shall have the meanings given in the Service Agreement.

This Section "Defined Terms" shall be interpreted in conjunction with Annex VI (Jurisdiction Specific Terms).

2. DATA PROCESSING OBLIGATIONS

2.1 Relationship

(a) Alemira as a Processor of Customer Content: Customer and Alemira agree that with regard to the processing of Customer Content generated using Services listed in Annex III as applicable, Customer shall act either as a Controller or Processor and Alemira shall act as a Processor. As Processor, Alemira shall only process the Personal Data of Customer for the purposes set forth in the Service Agreement and/or according to Customer's written instructions unless required to process Customer personal data for other purposes according to the Applicable Law to which Alemira is subject; in such a case, Alemira shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Service Agreement (including this DPA) constitutes such initial written instructions by Customer.

(b) Alemira as a Controller of Customer Content: Customer and Alemira agree that with regard to the processing of Customer Content generated using Services listed in Annex III as applicable, Alemira is an independent Controller of Customer Content. Alemira will process Customer Content as an independent Controller in order to process the data for its own purposes e.g. to produce aggregated statistics for Service improvement, create tailored offers or provide insights into the efficiency of courses, assessments and similar feedback as applicable. As an independent Controller, Alemira shall solely determine the purposes and means of processing.

(c) Alemira as a Controller of Customer Account Data: Customer and Alemira acknowledge that, with regard to the processing of Customer Account Data, Customer is a Controller and Alemira is an independent Controller, not a Joint Controller with Customer. Alemira will process Customer Account Data as a Controller in order to (i) manage the relationship with Customer; (ii) carry out Alemira's

core business operations, such as accounting and filing taxes if applicable; (iii) detect, prevent, and/or investigate security incidents, fraud, and other abuse or misuse of the Services; (iv) perform identity verification; (v) comply with Alemira's legal or regulatory obligation to retain Subscriber Records; and (vi) as otherwise permitted under Applicable Data Protection Law and in accordance with this DPA, the Service Agreement, and the Alemira Privacy Notice.

(d) Alemira as a Controller of Customer Usage Data: The parties acknowledge that, regarding the processing of Customer Usage Data, Customer shall act either as a Controller or Processor and Alemira shall act as an independent Controller, not a Joint Controller with Customer. Alemira will process Customer Usage Data as a Controller for the purpose of carrying out the necessary functions as a service provider, such as: (a) Alemira's accounting, tax, billing, audit, and compliance purposes as applicable; (b) to provide, optimize, and maintain the Services, platform and security; (c) to investigate fraud, wrongful or unlawful use of the Services; (d) as required by applicable law; or (e) as otherwise permitted under Applicable Data Protection Law and in accordance with this DPA, the Service Agreement, and the Alemira Privacy Notice.

2.2. Purpose Limitation

(a) Alemira will process personal data in order to provide the Services in accordance with the Service Agreement. Annex I (Details of Personal Data Processing) of this DPA further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of personal data and the categories of data subjects.

(b) Customer appoints Alemira as a Processor to process Customer Content on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Service Agreement, this DPA, and as otherwise necessary to provide the Services to Customer, and which includes investigating security incidents and preventing fraudulent activity, and violations of the Alemira Privacy Notice, the current version of which is available at https://www.constructor.tech/privacy-policy and detecting and preventing service exploits or abuse; (b) as necessary to comply with Applicable Laws including Applicable Data Protection Law; and (c) as otherwise agreed in writing between Customer and Alemira (henceforth, "Permitted Purposes").

2.3 Obligations and Rights of the Parties

(a) Customer hereby warrants and represents, on a continuous basis throughout the Term of the Service Agreement, that all Personal Data provided or made available by Customer to Alemira for processing pursuant to the Service Agreement has been lawfully collected by Customer and transferred to Alemira in compliance with Data Protection Laws. During the Term of this DPA, Customer is solely responsible for obtaining and maintaining all necessary approvals, consents, authorizations and licenses from each and every Data Subject as required under Data Protection Laws to enable Alemira to process the Personal Data pursuant to the Service Agreement and DPA and to exercise its rights and fulfil its obligations under this DPA.

(b) Customer will ensure that its instructions as per Section 2.2.Purpose Limitation) comply with Applicable Data Protection Law. Customer acknowledges that Alemira is neither responsible for determining which laws or regulations are applicable to Customer's business nor whether Alemira's provision of the Services meets or will meet the requirements of such laws or regulations. Customer will ensure that Alemira's processing of Customer Content, when done in accordance with Customer's instructions, will not cause Alemira to violate any Applicable Law or regulation, including Applicable Data Protection Law.

(c) Unless restricted by Applicable Law, Alemira shall inform Customer if, in Alemira's opinion, any processing under the Service Agreement or an instruction by Customer regarding the processing of the Personal Data according to the Service Agreement and/or the written instructions of Customer conflicts with Alemira's legal obligations or the Applicable Law. Upon informing the Customer, Alemira shall discontinue the processing of Personal Data under this DPA in compliance with its legal obligations and Applicable Law. In such case, Alemira and Customer will mutually agree on a solution based on the terms of the Service Agreement read together with the terms of this DPA in observance of the Applicable Law.

(d) Alemira shall treat all Personal Data as confidential and shall ensure that all employees, agents and Sub-Processors authorized by Alemira to process Personal Data are subject to contractual obligations of confidentiality that will survive the Term of the Service Agreement

(e) Alemira shall provide Customer with reasonable assistance with Data Protection Impact Assessments or prior consultations with data protection authorities that Customer is required to carry out under Data Protection Laws. Any such assistance shall be as agreed between the Parties and could be subject to a mutually accepted fee.

(f) Alemira shall implement appropriate technical and organizational measures in relation to the processing of Personal Data intended to ensure a level of security appropriate to the Personal Data processing, including, as applicable, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Personal Data and a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data. Both Parties hereby acknowledge and agree that the security measures available at https://constructor.tech/technical-organizational-measures provide appropriate and sufficient safeguards according to Applicable Law for the processing of Personal Data pursuant to the Service Agreement. Alemira may update these security measures, which will in every case provide an appropriate and sufficient level of security, according to Applicable Law and will inform Customer of substantial changes thereof.

(g) After becoming aware with a reasonable degree of certainty of the occurrence of an accidental or unlawful Data Breach concerning the Personal Data transmitted, stored or otherwise processed by Alemira under this DPA, Alemira shall notify Customer of the Data Breach without undue delay as set forth in records stored by Alemira on the Customer as contact details. Alemira will provide such information as Customer may reasonably require meeting its obligations under Applicable Law with respect to the Data Breach and take reasonable steps to contain and remediate the Data Breach. Alemira may provide such information in phases as it becomes available. For the avoidance of doubt, a notification of the Data Breach by Alemira shall not be construed or interpreted as an admission of fault or liability by Alemira.

(h) Alemira shall promptly notify Customer upon receiving any complaint, notice or communication relating to the processing of Personal Data under this DPA. At Customer's request and expense, Alemira shall provide Customer with reasonable co-operation and assistance required by Customer in order to fulfill its obligations under Applicable Law in relation to any requests from Third Parties. Alemira will not respond to any Third Party Request without Customer's prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Customer.

(i) Insofar as Customer is subject to an audit or investigation from a competent data protection authority Alemira shall, when required, respond to any information requests, and/or agree to submit its premises and operations to audits, including inspections by Customer and/or the competent data

protection regulator, in each case for the purpose of evidencing its compliance with this DPA, provided that:

i. Customer shall ensure that all information obtained or generated in connection with any information request, audit or inspection is kept strictly confidential as per Applicable Law;
ii. Customer shall ensure that any information request, audit or inspection is undertaken within normal business hours (unless such other time is mandated by a competent data protection authority) with minimal disruption to Alemira's business.
iii. Such information request, audit or inspection shall not oblige Alemira to provide or permit access to information concerning Alemira's confidential company information or information relating to other customers of Alemira;
iv. In the event of a request, audit or inspection concerning Alemira, Customer shall be subject to any reasonable policies, procedures or instructions of Alemira for the purposes of preserving security and confidentiality of its data and premises;
v. Customer shall give Alemira at least 30 days' prior written notice of an information request and/or audit or inspection unless the competent data protection regulator provides Customer with less than 30 days' notice, in which case Customer shall inform Alemira immediately and without undue delay.
vi. If any information request, audit or inspection relates to systems provided by or on the premises of Alemira's Sub-Processors, the scope of such information request, audit and/or inspection shall be as permitted under the relevant agreement in place between Alemira and the concerned Sub-Processor.
vii. A maximum of one information request, audit and/or inspection may be requested by Customer in any twelve (12) month period unless an additional information request, audit and/or inspection is mandated by a competent data protection authority in writing.
viii. Customer shall bear all information request, audit and/or inspection costs and reimburse Alemira for all costs incurred in relation to the same and for Alemira's support of the request, audit and/or inspection.
ix. Where Customer engages third parties to perform the DPIA or the audit, Customer selects such third parties that are qualified to perform the DPIA or the audit, do not compete with Alemira, and are legally bound to confidentiality with respect to Data Sub-Processor's confidential data.

(j) Upon expiration or any earlier termination of the Service Agreement, or upon Customer's written request, Alemira shall delete all Customer Personal Data in Alemira's possession unless Alemira is required to retain Customer Personal Data to comply with its obligations under Applicable Law. Alemira shall notify all relevant Sub-Processors of the obligation to delete all Customer Personal Data in their possession upon expiration or any earlier termination of the Service Agreement, or upon Customer's written request. Sub-Processors will be mandated to delete all Customer Personal Data according to their obligations under the DPA concluded between such Sub-Processors and Alemira in the terms of Section 3. SUB-PROCESSORS) below.

(k) Subject to this DPA and the requirements of Applicable Data Protection Law, Alemira shall exercise its own discretion in the selection and use of means necessary to perform its processing obligations under the Service Agreement.

2.4. Additional Instructions

Additional instructions outside the scope of the Service Agreement or this DPA will be agreed to in writing between Customer and Alemira, including any additional fees that may be payable by Customer to Alemira for carrying out such additional instructions.

3. SUB-PROCESSORS

(a) Customer hereby provides its general authorization to Alemira to appoint the Sub -Processors set forth on in Annex III as of the Effective Date of this DPA to process Personal Data on Alemira's behalf. Alemira shall ensure that the same data protection obligations as set out in this DPA are contractually imposed on its Sub-Processors, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Applicable Laws.

(b) Alemira shall notify Customer of any amendments effected on the Alemira Sub-Processor List by sending a notification to the Customer using the contact details stored by Alemira on the Customer. Customer may object to any such amendment by email no later than fifteen (15) days after the date of the notification, provided that Customer has a legitimate reason to object according to Applicable Laws. If the Parties cannot mutually agree on a reasonable resolution to Customer's objection, either Party may terminate the Service Agreement upon written notice to the other Party.

(c) Customer shall inform Alemira in writing in advance of the expected processing of sensitive data by Alemira, which requires specific restrictions and additional safeguards during processing.

(d) Customer may object to Alemira's appointment or replacement of a Sub-Processor provided such objection is in writing and based on reasonable grounds according to Applicable Law. In such an event, Customer and Alemira agree to discuss commercially reasonable alternative solutions in good faith. If Customer and Alemira cannot reach a resolution within ninety (90) days from the date of Alemira's receipt of Customer's written objection, Customer may discontinue the use of the affected Services by providing written notice to Alemira. Such discontinuation will be without prejudice to any fees incurred by Customer prior to the discontinuation of the affected Services. If no objection has been raised against Alemira replacing or appointing a new Sub-Processor, Alemira will deem Customer to have authorized the new Sub-Processor.

4. DATA SUBJECT RIGHTS

Alemira provides Customer with a number of features via the Services, including the ability to delete, obtain a copy of, or restrict use of Customer Content. Customer may use such features to assist in complying with its obligations under Applicable Law with respect to responding to Third Party Requests from data subjects via the Services at no additional cost. Upon Customer's request, Alemira will provide reasonable additional and timely assistance to Customer in complying with Customer's data protection obligations with respect to data subject rights under Applicable Law to the extent Customer does not have the ability to resolve a Third Party Request from a data subject through features made available via the Services.

5. LIABILITY

Applicable Law will govern liability.

6. INTERNATIONAL TRANSFERS

(a) To the extent Alemira processes personal data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in Annex VI (Jurisdiction Specific Terms) of this DPA,

the terms specified in Annex VI with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

(b) To the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area, Switzerland, or any other jurisdiction listed in Annex VI (Jurisdiction Specific Terms) of this DPA to Alemira located outside of that jurisdiction, the terms set forth in Annex V (Cross Border Transfer Mechanisms) of this DPA will apply.

8. MISCELLANEOUS

(a) In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms set forth in Annex VI(Jurisdiction Specific Terms) of this DPA; (2) the terms of this DPA outside of Annex VI(Jurisdiction Specific Terms); (3) the Service Agreement; and (4) the Alemira Privacy Notice (https://constructor.tech/privacy-policy). Any claims brought in connection with this DPA will be subject to the terms and conditions, including, without limitation, the exclusions and limitations set forth in the Service Agreement.

(b) Alemira may update the terms of this DPA from time to time; provided, however, Alemira will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services.

(c) English shall be used as the authoritative text, regardless of the possible existence of counterparts translated into another language.

(d) Each Party shall be liable to the other Party for any damages it causes to the other Party by any breach of this DPA or Applicable Laws on personal data protection.

(e) Except as amended by this DPA, the terms of the Service Agreement shall remain in full force and effect. Any claims arising under this DPA shall be subject to the exclusions, limitations and other terms of the Service Agreement. If the Service Agreement and this DPA conflict, then this DPA shall prevail but solely with respect to the terms related to the processing of Personal Data. This DPA shall expire on the expiration or any earlier termination of the Service Agreement or the date on which Alemira no longer processes Personal Data, whichever is earlier.

ANNEX I

DETAILS OF PERSONAL DATA PROCESSING ACCORDING TO ART. 28(3) GDPR

1. NATURE AND PURPOSE OF THE PROCESSING

Alemira will process Personal Data as necessary to provide the Services under the Service Agreement as detailed in Annex III acting as a Controller or Processor according to Section 2.1 Relationship) of this DPA.

2. PROCESSING ACTIVITIES

Customer Content, Customer Account Data and Customer Usage Data will be collected, stored and used by Alemira in order to provide customizable services to Customer:

- Customer will receive customizable services related to learning and research.
- Customer will be given access to web-based applications and infrastructure and access to services facilitating synchronous data sharing.
- Customer will receive analytic reports depending on the chosen Service containing Personal Data and/or aggregated data regarding the engagement of learners, their individual development, test and exam results, as well as analysis on participation and interest in courses, as applicable according to the Service.
- Customer will receive an analysis and evaluation of behavioral and environmental data collected from data subjects against a set of expectations leading to the assessment on personal development on a given subject, such as reading, writing, mathematical skills or a score achieved during an exam.

Customer solely decides on integrating, managing and controlling its data relating to either end users or other participants such as research project members as applicable according to the chosen Service.

3. DURATION OF THE PROCESSING

The period for which personal data will be retained and the criteria used to determine that period are as follows:

3.1 Customer Content

Prior to the termination of the Service Agreement, Alemira will process stored Customer Content for the Permitted Purposes as per 2.2. Purpose Limitation) until Customer elects to delete such Customer Content using the features via the Services. Customer agrees that it is solely responsible for deleting Customer Content via the Services.

Upon termination of the Service Agreement, at the choice of the Customer, Alemira will delete or return all the personal data to the Customer after the end of the provision of services relating to processing and will delete existing copies unless the Applicable Law requires storage of the Personal Data.

3.2 Customer Account Data

Alemira will process Customer Account Data as long as required,

(a) to provide the Services to Customer;

(b) for Alemira's legitimate business needs; or,

(c) by applicable law or regulation.

3.3 Customer Usage Data

Upon termination of the Service Agreement, Alemira may retain, use, and disclose Customer Usage Data for the purposes set forth in 2.1 Relationship) of this DPA, subject to the confidentiality obligations set forth in the Service Agreement. Alemira will anonymize or delete Customer Usage Data when Alemira no longer requires it for the purposes set forth in 2.1 Relationship) of this DPA.

4. CATEGORIES OF DATA SUBJECTS

4.1 Customer Content

- Customer's end users;
- Permitted users of Alemira.

4.2 Customer Account Data

- Customer's employees;
- Individuals authorized by Customer to access Customer's Alemira account;
- Permitted users of Alemira.

4.3 Customer Usage Data

- Customer's end users;
- Permitted users of Alemira.

5. CATEGORIES OF PERSONAL DATA.

Personal data of Customer's employees: name, address, contact data stored in Alemira's records.

Personal data of Customer's end users and Permitted users:

Digital profile: user ID, username, password, profile photo, contact information (e-mail address, name, surname, phone numbers), educational content, email replies and answers, device-specific and operating system data;

Data from the use of the Service(s) as applicable: IP address, audit logs, browser type and language, time zones, date and time of your request and referral URLs, cookies, settings preferences, scores, performance results, learning results, achievements, certificates, enrolled and passed courses, configuration data, educational history, proof of identity (identity card, passport), photographic and video imaging, eye tracking, educational trajectory, course topic mapping, logs of interaction with the service, decision making data, configuration data.

6. SPECIAL CATEGORIES OF DATA

Special Categories of Data may, from time to time, be processed via the Services where Customer or its end users choose to include Special Categories of Data e.g. health data within the data that are transmitted using the Services. Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Customer's end users to transmit or process, any Sensitive Data via the Services. Customer is responsible for collecting explicit consent from users before processing special categories of data.

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES

Alemira will maintain appropriate and sufficient technical and organizational measures to ensure the security, confidentiality and integrity of Personal Data processed pursuant to the Service Agreement as described at https://constructor.tech/technical-organizational-measures.

Alemira AG contractually requires all Sub-Processors to implement technical and organizational measures at least equivalent to, and in any case no less protective than those referenced above.

ANNEX III

DESCRIPTION OF THE SERVICES

Services where Alemira is a Processor:	
Proctor	Proctor is a technology that analyses online user behaviour based on facial recognition and emotion detection. Proctored examination includes students' authentication, audio and video feeds of the monitor screen and a web camera and, if required, the following proctor services to check if any violations existed (such as an attempt to cheat the system, help of another person, for example, the use of other devices and such).
Learning Management System	LMS is a web-based platform for creating, delivering, and analyzing online courses. This service is supported by a collection of autonomous web services called independently deployed applications (IDAs).
Assessment	Assessment is a technology for organisations who need to provide and assess questions in their educational process. Alemira Active Assessment is an assessment software allowing to create, store and update adaptive quizzes and questions, providing various assessment modes and authoring tools to manage quality and versions of questions
Research Platform	Research Platform is a powerful tool that provides scientists with all the capabilities to conduct a full research cycle. A project in the Research Platform is a combination of storage and computing resources allocated to a piece of science work (such as research or a survey), as well as of data that is to be studied and algorithms to process the data. Each project has its own folder in the local and cloud storages. The project data is committed to a cloud repository and shared among the project team members, which allows them to work collaboratively. During your work on the project, you can configure the virtual environment to meet your project requirements. Virtual environments can be changed from session to session, and different project members can use different virtual environments when working on the same shared project. The service includes a feature to publish articles on project findings and related results. Publications can be accessed publicly or only by members of the project team. Research Platform has a set of default virtual environment templates from which you can choose a template to run your project.
Infrastructure	This is a service of unified cloud infrastructure that is designed with ready-to-go configurations that provide unmatched support and service for education and research. Users can operate on-premises or in a private university cloud, all with a unified cloud approach. We offer public cloud-like experience while having sensitive data to remain inside. Services are customized to reflect established processes and can be integrated with existing SW solutions.
Classroom	A virtual classroom software that helps to prepare, run and analyze online and hybrid classes interactively. Students will be able to engage actively with their instructors and peers. Educators can create and deliver interactive learning

	experience. Rich annotation capabilities provide students with more succinct explanations. Provides insights that analyzes overall session engagement of students. With collaborative whiteboards and breakout rooms, students will be engaged in a vibrant discussion. Recorded classes can be reused, adjusted, reviewed with all files, session structure, discussions and annotations.
Coding / Virtual Labs	Labs are platforms for hands-on IT training. They can be used by end-users to accelerate software adoption by students, faculty, employees, partners. They have automatic assessment and semi-automatic lab authoring unique features. With them, both students and instructors could benefit from faster lab building and assessment.

Services where Alemira is a Controller:	
Avatar	Avatar is a digital, but photo-realistic representation of a human. Avatars can be used to create, customize, and use digital videos in various online environments, such as social media, virtual worlds, video games, chat applications, and more. One can create a custom avatar of themselves or of someone else. The production of visual and voice prototypes for the Avatar service is based on Alemira's Articifial Intelligence technology.
Brand Impact	The service consists of the analysis of key performance metrics to enhance the effectiveness of a sponsorship strategy. The brand Impact score (BIS) is calculated by MI-powered analytical tool, and it's based on the quality and duration of the brand exposure during an event's broadcast. A report analyzing multiple media channels is available almost immediately after the broadcast, providing comprehensive data about the value of brand visibility against the marketing investment.
Calcularis	Calcularis empowers all children, including those with learning disabilities and gifted children, to master the fundamentals of mathematics autonomously and effectively. Our training systems, Grafari and Calcularis are computer-based training systems. The systems automatically evaluate the trainees' input, i.e. their answers to the posed tasks, and so estimate individual difficulties and strengths of the trainees with respect to the writing and math tasks contained in the training systems. Based on these estimations, the systems compute individually optimized learning plans. Trainees can work on their own with the training applications, while their parents and/or educators can supervise and support them using the coaching applications.
Grafari	Grafari helps children learn and master spelling up to 6th grade. Grafari (Phonics) introduces writing skills, while Grafari (Orthograh) specifically emphasizes spelling practice. Our training systems, Grafari and Calcularis are computer-based training systems. The systems automatically evaluate the trainees' input, i.e. their answers to the posed tasks, and so estimate individual difficulties and strengths of the trainees with respect to the writing and math tasks contained in the training systems. Based on these estimations, the systems compute individually optimized learning plans. Trainees can work on their own with the training applications, while their parents and/or educators can supervise and support them using the coaching applications.
Race comms	Race Comms is a unique tool thoughtfully designed for professional racing to facilitate faster decision-making. It transforms traditional radio communication into a digital chat-like experience, making the monitoring process much smoother. The service includes real-time speech-to-text, communication clutter reduction, immediate feedback to developers, and custom dictionary.
Race lens	Race Lens is a cutting-edge tool specifically designed for the motorsports industry. It allows users to manage up to 100,000 images per event and enables real-time photo search, comparison, and analysis using advanced machine intelligence (MI) models.

ANNEX IV

LIST OF SUB-PROCESSORS

According to Section 3. SUB-PROCESSORS) of this DPA, as of the effective date of this DPA Customer provides its general authorization to Alemira AG to appoint

- Sub-processors listed on https://constructor.tech/subprocessors, and
- Sub-processors listed below belonging to the Alemira Group

to process Personal Data on behalf of Alemira:

Alemira Group sub-processors		
Alemira PTE Ltd. (8 Temasek boulevard, #30-01, Suntec Tower three, Singapore 038988)	Singapore	Access to data by local employees for the purposes of the Service Agreement
Alemira Software Limited (1700 Sofia, Studentski administrative district, 59 G.M. Dimitrov Blvd., “NV Tower” building, 11th floor, Bulgaria)	Bulgaria	Access to data by local employees for the purposes of the Service Agreement
Constructor Turkey Teknoloji Ve Egitim Hizmetleri Anonim Şirketi (Ergenekon Mah.Halaskargazİ Cad.No:51 İc Kapi No:4 Şisli)	Turkey	Access to data by local employees for the purposes of the Service Agreement
Dybuster AG (Lintheschergasse 7, 8001 Zürich, Switzerland)	Switzerland	Access to data by local employees for the purposes of the Service Agreement
Constructor Business Services LLC Belgrade, seat at Kneza Mihaila 33, II floor, Belgrade – Stari grad, company number 21779938, TIN 112971812	Serbia	Access to data by local employees for the purposes of the Service Agreement

ANNEX V

CROSS-BORDER DATA TRANSFER MECHANISMS

1. DEFINITIONS

- "EEA" means the European Economic Area
- "EU Standard Contractual Clauses" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914[1].
- "UK International Data Transfer Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.
- "EU-US Adequacy decision" means the adequacy decision adopted by the European Commission in 2023 related to the transfers of personal data between EU-US under the Data Privacy Framework.
- "Data Privacy Principles" means the Data Privacy Framework principles (as supplemented by the Supplemental Principles).

2. CROSS BORDER DATA TRANSFER MECHANISMS

2.1. Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of Personal Data will be subject to a single Transfer Mechanism, as applicable, and in accordance with the following order of precedence: (a) an adequacy decision granted by the European Commission as detailed here2 (b) the EU Standard Contractual Clauses as set forth in Section 2.3 (EU Standard Contractual Clauses) of this Annex V; (c) the EU Standard Contractual Clauses as modified and applicable under the Swiss data protection law (d) the UK International Data Transfer Addendum as set forth in Section 2.10 of this Annex V; and, if neither (a), (b), (c), (d) is applicable, then (e) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

2.2. EU-US Adequacy decision: To the extent that Customer is located in the United States of America and is self-certified under the Data Privacy Framework Alemira further agrees (i) to provide at least the same level of protection to any personal data as required by the Data Privacy Principles; (ii) upon written notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of personal data. The same will apply to Sub-Processors certified under the Data Privacy Framework. Customer agrees to notify Alemira in writing, without undue delay, if its self-certification to the Data Privacy Framework is withdrawn, terminated, revoked, or otherwise invalidated (in which case, an alternative Transfer Mechanism will apply in accordance with the order of precedence in Section 2.1 (Order of Precedence) of this Annex V.

2.3. EU Standard Contractual Clauses. The EU Standard Contractual Clauses3 will apply to Personal Data that is transferred for the purpose of providing the Services according to the Service

[1] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

[2] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacydecisions_en#:~:text=The%20European%20Commission%20has%20so,commercial%20organisations%20participating%20in%20the

[3] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

Agreement and this DPA from the EEA and/or Switzerland (s. Annex VII), either directly or via onward transfer, to any country or recipient outside the EEA and/or Switzerland that is not recognized by the relevant competent authority as providing an adequate level of protection of Personal Data. For data transfers that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into, and incorporated into this DPA by reference, and completed as applicable according to Section 2.1 of this DPA

2.4. For each Module, where applicable:

i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-processor changes will be as set forth in Section 3. SUB-PROCESSORS);

iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

iv) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Swiss law;

v) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland;

vi) in Annex I, Part A of the EU Standard Contractual Clauses:

2.5. Data Exporter: Customer

2.6. Contact details: The email address(es) designated by Customer in Customer's account via its notification preferences.

2.7. Data Exporter Role: The Data Exporter's role is set forth in Section 2.1 (Relationship) of this DPA.

2.8. Signature and Date: By entering into the Service Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the Service Agreement.

2.9. Data Importer: Alemira

i) Contact details: Alemira Privacy Team - privacy@constructor.tech

ii) Data Importer Role: The Data Importer's role is set forth in Section 2.1 (Relationship) of this DPA.

iii) Signature and Date: By entering into the Service Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Service Agreement;

iv) (vii) in Annex I, Part B of the EU Standard Contractual Clauses:

v) The categories of data subjects are set forth in Section 4 of Annex I (Details of Personal Data Processing According to Art. 28(3) GDPR) of this DPA.

vi) The Special Categories of data transferred is set forth in Section 6 of Annex I (Details of Personal Data Processing According to Art. 28(3) GDPR) of this DPA.

vii) The frequency of the transfer is a continuous basis for the duration of the Service Agreement.

viii) The nature of the processing is set forth in Section 1 of Annex I (Details of Personal Data Processing According to Art. 28(3) GDPR) of this DPA.

ix) The purpose of the processing is set forth in Section 1 of Annex I (Details of Personal Data Processing According to Art. 28(3) GDPR) of this DPA.

x) The period for which the Personal Data will be retained is set forth in Section 3 of Annex I (Details of Personal Data Processing According to Art. 28(3) GDPR) of this DPA.

xi) For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth in Annex IV.

xii) in Annex I, Part C of the EU Standard Contractual Clauses: The Federal Data Protection and Information Commissioner (FDPIC) of Switzerland will be the competent supervisory authority; and,

xiii) Annex II (Technical and Organizational Security Measures) of this DPA serves as Annex II of the EU Standard Contractual Clauses.

2.10. UK International Data Transfer Addendum. Customer and Alemira agree that the UK International Data Transfer Addendum (Annex VIII) will apply to personal data covered by UK data protection law that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Addendum, the UK International Data Transfer Addendum will be deemed entered into, and incorporated into this DPA in Annex VIII.

2.11. Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or the EU Standard Contractual Clauses as modified per the Swiss law or the UK International Data Transfer Addendum and any other terms in this DPA, including Annex VI (Jurisdiction Specific Terms), the Service Agreement, or the Alemira Privacy Notice, the provisions of the EU Standard Contractual Clauses or the EU Standard Contractual Clauses as modified per the Swiss law or UK International Data Transfer Addendum, as applicable, will prevail.

ANNEX VI

JURISDICTION SPECIFIC TERMS

1. AUSTRALIA:

1.1 The definition of “Applicable Data Protection Law” includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.

1.3 The definition of “Sensitive Data” includes “Sensitive Information” as defined under Applicable Data Protection Law.

2. BRAZIL:

2.1 The definition of “Applicable Data Protection Law” includes the Lei Geral de Proteção de Dados (General Personal Data Protection Act).

2.2 The definition of “Security Incident” includes a security incident that may result in any relevant risk or damage to data subjects.

2.3 The definition of “Processor” includes “operator” as defined under Applicable Data Protection Law.

3. CANADA:

3.1 The definition of “Applicable Data Protection Law” includes the Federal Personal Information Protection and Electronic Documents Act.

3.2 Alemira’s Sub-Processors, as set forth in Annex IV: List of Sub-Processors of this DPA, are third parties under Applicable Data Protection Law, with whom Alemira has entered into a written contract where the same data protection obligations as set out in this DPA are contractually imposed on such Sub-Processors. Alemira has conducted appropriate due diligence on its Sub-Processors.

3.3 Alemira will implement technical and organizational measures as set forth in Annex II: Technical and Organizational Measures of this DPA.

4. European Economic Area (EEA):

4.1 The definition of “Applicable Data Protection Law” includes the General Data Protection Regulation (EU 2016/679) (“GDPR”).

4.2 When Alemira engages a Sub-Processor under Annex IV: List of Sub-Processors of this DPA, it will:

(a) require any appointed Sub-Processor to protect personal data to the standard required by Applicable Data Protection Law, contractually imposing the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and,

(b) require any appointed Sub-Processor to (i) agree in writing to only process Personal Data in a country having been granted an adequacy decision by the Commission, or (ii) only process Personal Data subject to the terms of Chapter V GDPR.

4.3 Notwithstanding anything to the contrary in this DPA or in the Service Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

4.4 Customer acknowledges that Alemira, as a Controller, may be required under the Applicable Data Protection Law to notify a regulatory authority of Data Breaches involving Personal Data. If a regulatory authority requires Alemira to notify impacted data subjects with whom Alemira does not have a direct relationship (e.g., Customer's end users), Alemira will notify Customer of this requirement. Customer will provide reasonable assistance to Alemira to notify the impacted Data Subjects.

5.ISRAEL:

5.1 The definition of "Applicable Data Protection Law" includes the Protection of Privacy Law.

5.2 The definition of "Controller" includes "Database Owner" as defined under Applicable Data Protection Law.

5.3 The definition of "Processor" includes "holder" as defined under Applicable Data Protection Law.

5.4 Alemira will require that any personnel authorized to process personal data comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Law. Such personnel shall be bound to a duty of confidentiality in accordance with Section 2.3 Obligations and Rights of the Parties) of this DPA.

5.5 Alemira must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Annex II: Technical and Organizational Measures of this DPA and complying with the terms of the Service Agreement.

5.6 Alemira must ensure that Customer Personal Data will not be transferred to a Sub-Processor unless such Sub-Processor has executed an agreement with Alemira pursuant to Section 3. SUB-PROCESSORS) of this DPA.

6. MEXICO:

6.1 The definition of "Applicable Data Protection Law" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations.

6.2 When acting as a Processor, Alemira will:

(a) Process Personal Data in accordance with Customer's instructions set forth in Section 2.2. Purpose Limitation) of this DPA;

(b) Process Personal Data only to the extent necessary to provide the Services;

(c) implement security measures in accordance with Applicable Data Protection Law and Section 2.3 Obligations and Rights of the Parties) of this DPA;

(d) keep confidentiality regarding the Personal Data Processed in accordance with the Service Agreement;

(e) delete all Personal Data upon termination of the Service Agreement in accordance with Section 2.3 Obligations and Rights of the Parties) of this DPA; and,

(f) only transfer personal data to Sub-Processors in accordance with Section 3. SUB-PROCESSORS) of this DPA.

7. Singapore:

7.1 The definition of “Applicable Data Protection Law” includes the Personal Data Protection Act 2012 (“PDPA”).

7.2 Alemira will process Personal Data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Section 2.3 Obligations and Rights of the Parties) of this DPA and complying with the terms of the Service Agreement.

8. SWITZERLAND:

8.1 The definition of “Applicable Data Protection Law” includes the Swiss Federal Act on Data Protection, as revised (“revFADP”).

8.2 When Alemira engages a Sub-Processor under Section 3. SUB-PROCESSORS) of this DPA, it will:

(a) require any appointed Sub-Processor to protect the Customer Personal Data to the standard required by Applicable Data Protection Law, such as contractually imposing on such Sub-Processor the same data protection obligations referred to in Article 28(3) of the GDPR, in particular, providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and,

(b) require any appointed Sub-Processor to (i) agree in writing to only process Personal Data in a country that Switzerland has declared to have an “adequate” level of protection or (ii) only process Personal Data on the terms prescribed by Chapter V GDPR.

8.3 To the extent that Personal Data transfers from Switzerland are subject to the EU Standard Contractual Sections in accordance with Section 2.3 of Annex V (EU Standard Contractual Clauses), the following amendments will apply to the EU Standard Contractual Clauses as illustrated in Annex VII:

(a) references to “EU Member State” and “Member State” will be interpreted to include Switzerland, and,

(b) insofar as the transfer or onward transfers are subject to the revFADP:

(i) references to "Regulation (EU) 2016/679" are to be interpreted as references to the revFADP;

(ii) the “competent supervisory authority” in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

(iii) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and,

(iv) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.

9. UNITED KINGDOM (UK):

9.1 References in this DPA to “GDPR” will be deemed references to the corresponding laws and regulations of the United Kingdom, including, without limitation, the UK GDPR and Data Protection Act 2018.

9.2 When Alemira engages a Sub-Processor under Section 3. SUB-PROCESSORS) of this DPA, it will:

(a) require any appointed Sub-Processor to protect the Customer Personal Data to the standard required by Applicable Data Protection Law, such as contractually imposing on such Sub-Processor the same data protection obligations referred to in Article 28(3) of the GDPR, in particular, providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and,

(b) require any appointed Sub-Processor to (i) agree in writing to only process Personal Data in a country that the United Kingdom has declared to have an “adequate” level of protection or (ii) only process Personal Data on terms equivalent to the UK International Data Transfer Addendum or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

9.3 Notwithstanding anything to the contrary in this DPA or in the Service Agreement (including, without limitation, either party’s indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party’s violation of the UK GDPR.

9.4 Customer acknowledges that Alemira, as a Controller, may be required under Applicable Data Protection Law to notify a regulatory authority of Data Breaches involving Customer Personal Data. If a regulatory authority requires Alemira to notify impacted data subjects with whom Alemira does not have a direct relationship (e.g., Customer’s end users), Alemira will notify Customer of this requirement. Customer will provide reasonable assistance to Alemira to notify the impacted data subjects.

10. UNITED STATES OF AMERICA:

10.1 “US State Privacy Laws” means all state laws relating to the protection and processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“CCPA”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

10.2 The definition of “Applicable Data Protection Law” includes US State Privacy Laws.

10.3 The following terms apply where Alemira processes personal data subject to the CCPA:

(a) The term “personal information”, as used in Section 10.3 of this Annex VI, will have the meaning provided in the CCPA;

(b) Alemira is a service provider when processing Personal Data. Alemira will process any personal information only for the business purposes set forth in the Service Agreement, including the purpose of processing and processing activities set forth in this DPA . As a service provider, Alemira will not sell or share Customer Content or retain, use, or disclose Customer Content (i) for any purpose other

than the Purpose, including retaining, using, or disclosing Customer Content for a commercial purpose other than the Purpose, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Alemira;

(c) Alemira will (i) comply with obligations applicable to it as a service provider under the CCPA and (ii) provide personal information with the same level of privacy protection as is required by the CCPA. Customer is responsible for ensuring that it has complied, and will continue to comply, with the requirements of the CCPA in its use of the Services and its own processing of personal information;

(d) Customer will have the right to take reasonable and appropriate steps to help ensure that Alemira uses personal information in a manner consistent with Customer's obligations under the CCPA;

(e) Alemira will notify Customer if it makes a determination that it can no longer meet its obligations as a service provider under the CCPA;

(f) Upon notice, Customer will have the right to take reasonable and appropriate steps in accordance with the Service Agreement to stop and remediate unauthorized use of personal information;

(g) Alemira will provide reasonable and timely assistance to assist Customer in complying with its obligations with respect to consumer requests as set forth in the Service Agreement;

(h) For any Sub-Processor engaged by Alemira to process personal information subject to the CCPA, Alemira will ensure that Alemira's agreement with such Sub-Processor complies with the CCPA, including, without limitation, the contractual requirements for service providers and contractors;

(i) Alemira will not combine Customer Content that it receives from, or on behalf of, Customer, with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, unless such combination is required to perform any business purpose as permitted by the CCPA, including any regulations thereto, or by regulations adopted by the California Privacy Protection Agency; and,

(j) Alemira certifies that it understands and will comply with its obligations under the CCPA.

ANNEX VII

LOCALIZATION OF THE EU STANDARD CONTRACTUAL CLAUSES TO SWISS LAW

For the purposes of localizing the Standard Contractual Clauses to comply with the revFADP, the parties agree to the following:

(1) The parties adopt the GDPR standard for all data transfers.

(2) The term "personal data" shall include personal data as defined under the revised Federal Act on Data Protection. The list of data subjects and categories of data in relation to the Standard Contractual Clauses shall not be deemed to restrict the application of the Standard Contractual Clauses to personal data which is subject to this clause.

(3) References to (articles in) the EU General Data Protection Regulation 2016/679 shall be deemed to refer to (respective articles in) the revFADP.

(4) Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Federal Data Protection and Information Commissioner and, concurrently, the EEA member state authority identified above.

(5) Clause 17: the parties agree that the governing jurisdiction is Switzerland.

(6) Clause 18: replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of Switzerland. The parties agree to interpret the Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(c).

(7) The parties agree to interpret the Standard Contractual Clauses so that "Data Subjects" includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.

(8) References to Member State(s)/EU Member State(s)/EU/Union shall be deemed to refer to Switzerland.

(9) Reference to the exporter in the EU shall be deemed to refer to the exporter in Switzerland.

(10) Reference to the European Union shall be deemed to refer to Switzerland.

(11) Where the Clauses use terms that are defined in the EU General Data Protection Regulation 2016/679, those terms shall be deemed to have the meaning as the equivalent terms are defined in the revFADP.

ANNEX VIII

UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

In reference to the DPA made by and between the Parties set out at the beginning of the DPA**,** such DPA includes the UK Addendum as follows:

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum issued by the Information Commissioner, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.
3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs.
4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfills the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws apply.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.
9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this DPA incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.
12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 11, the provisions of Section 14 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 11 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 11) are made:

a) References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b) In Clause 2, delete the words:
"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c) Clause 6 (Description of the transfer(s)) is replaced with:
"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d) Clause 8.7(i) of Module 1 is replaced with:
"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e) Clause 8.8(i) of Modules 2 and 3 is replaced with:
"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g) References to Regulation (EU) 2018/1725 are removed;

h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j) Clause 13(a) and Part C of Annex I are not used;

k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l) In Clause 16(e), subsection (i) is replaced with:
"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m) Clause 17 is replaced with:
"These Clauses are governed by the laws of England and Wales.";

n) Clause 18 is replaced with:
"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
    a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b) reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
    a) its direct costs of performing its obligations under the Addendum; and/or
    b) its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.
21. The Parties hereby, acknowledge that SCHEDULE D shall be updated for transfers from the UK to countries outside the EEA shall be fully bound by, and subject to, all the requirements provided by the updated references included within this AMENDMENT.

Table 1: Parties

Start date	See starting date of the Service Agreeement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer(s) (who receive the Restricted Transfer)**
Parties' details	Full legal name: Customer Main address (if a company registered address): As stated in the Service Agreement Official registration number (if any) (company number or	Full legal name: Alemira Main address (if a company registered address): As stated in the Service Agreement Official registration number (if any) (company number or similar identifier): As stated in the Service Agreement _____

	similar identifier): As stated in the Service Agreement	_____ Full legal name: Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signatures	See the signatures made above.	See the signatures made above.

Table 2: Selected SCCs, Modules and Selected Clauses[4]

Addendum EU SCCs	☒ **The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:** See Annex 5 and the references made therein to further Annexes. Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data

[4] Yellow areas mean that these Clauses do not exist under the corresponding Module.

				General Authorisation)		collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex 5.
Annex 1B: Description of Transfer: See Annex 5.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex 2.
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex 3

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Table 5: Terminology

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.

Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.