

DATA PROCESSING ADDENDUM

Company	Author	Version	Date
GamaLearn	Omar Rizk, CTO	01	25.06.2025

This SwiftAssess Data Processing Addendum (the ‘DPA’) forms part of the SwiftAssess [Terms and Conditions](#) (the ‘Terms’), the agreement between Client (hereinafter ‘Client’, ‘you’) and GamaLearn (hereinafter ‘Company’, ‘GamaLearn’, ‘SwiftAssess’, ‘we’, ‘us’, or ‘our’) which is governing the processing of personal data that Client uploads or otherwise provides GamaLearn in connection with the services or of any personal data that GamaLearn obtains in connection with the performance of services, or any other personal data with respect to which Client is a data controller or data processor and GamaLearn is a data processor, hereinafter referred to individually as a ‘Party’ or together as the ‘Parties’.

Unless otherwise defined in this DPA, all capitalised terms used in this DPA will have the meanings set forth in the SwiftAssess Terms and Conditions. This DPA shall remain in force until the termination or expiration of the Terms between Client and us governing the Client’s use of the Services and all Personal Data has been returned or deleted in accordance with the provisions of this DPA.

1. Definitions

“**Standard Contractual Clauses (SCC)**” means Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj.

“**General Data Protection Regulation (GDPR)**” means 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, and repealing Directive 95/46/EC.

“**Personal Data**” means any information relating to an identified or identifiable natural person.

“**Data Subject**” means the identified or identifiable person to whom Personal Data relates.

“**Client Personal Data**” means Personal Data that Client uploads or otherwise provides GamaLearn in connection with the services or of any personal data that GamaLearn obtains in connection with the performance of services, or any other personal data with respect to which Client is a data controller or data processor and GamaLearn is a data processor.

“**Other Data Protection Laws and Regulations**” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, the United States and its states, United Arab Emirates, Saudi Arabia, and Oman applicable to the processing of Personal Data under the Terms as amended from time to time, other than the GDPR.



“Sub-processor” means any entity which provides processing services to GamaLearn in furtherance of GamaLearn’s processing on behalf of Client.

“Public Authority” means a government agency or law enforcement authority, including judicial authorities.

“Supervisory Authority” means an independent public authority to be responsible for monitoring the application of the data protection legislation.

2. Roles and Responsibilities

If the GDPR or Other Data Protection Laws and Regulations apply to your processing of Client Personal Data, you acknowledge and agree that with regard to the processing of Client Personal Data, you are a controller or a processor and we are a processor (as defined by the GDPR or Other Data Protection Laws and Regulations) acting on your behalf, as further described in this DPA. This DPA shall not apply to situations where we act as a controller in accordance with GamaLearn’s Privacy Policy.

3. Instructions

The Parties agree that this DPA and the Terms constitute your complete and final documented instructions regarding our processing of Client Data on your behalf (the ‘**Instructions**’). Any additional or alternate instructions must be consistent with the terms and conditions of this DPA and the Terms.

4. Your Obligations

Within the scope of the DPA and Terms and your use of the Services, you will be solely responsible for complying with all requirements that apply to you under the GDPR and Other Data Protection Laws and Regulations. You represent and warrant that you will be solely responsible for:

- (i) the accuracy, quality, integrity, confidentiality and security of collected Client Data;
- (ii) complying with all necessary transparency, lawfulness, fairness and other requirements under GDPR and Other Data Protection Laws and Regulations for the collection and use of the personal data by:
 - establishing and maintaining the procedure for the exercise of the rights of the Data Subjects whose Client Personal Data are processed on behalf of Client;
 - providing us only with data that has been lawfully and validly obtained and ensuring that such data will be relevant and proportionate to the respective uses;
 - ensuring compliance with the provisions of this DPA and Terms by your personnel or by any third-party accessing or using Client Personal Data on your behalf.
- (iii) ensuring that your Instructions to us regarding the processing of Client Data comply with the GDPR and Other Data Protection Laws and Regulations, including complying with principles of data minimisation, purpose and storage limitation; and
- (iv) complying with all applicable laws, rules, regulations (including GDPR and Other Data Protection Laws and Regulations) in respect to any Instructions you issue to us.

5. Our Obligations

5.1. General Obligations.

With regard to the processing of Personal Data GamaLearn shall:

- (i) process Client Personal Data only for the purpose of providing the services, using appropriate technical and organisational security measures, and in compliance with the instructions received from Client subject to Sections 3 and 4 of this DPA;



(ii) inform Client if GamaLearn cannot comply with its obligations under this DPA, in which case Client may terminate the Agreement or take any other reasonable actions, including suspending data processing operations;

(iii) inform Client if, in GamaLearn's opinion, a Client's Instruction may be in violation of the provisions of the GDPR or Other Data Protection Laws and Regulations;

(iv) follow Client's instructions regarding the collection of Client Personal Data (including with regard to the provision of notice and exercise of choice), in case GamaLearn is obtaining Client Personal Data from Data Subjects on behalf of Client under Terms;

(v) take reasonable steps to ensure that any employee/contractor to whom GamaLearn authorises access to Client Data on its behalf comply with respective provisions of the Terms and this DPA.

5.2. Notices to Client.

Upon becoming aware, we shall inform you of any legally binding request for disclosure of Client Personal Data by a Public Authority, unless GamaLearn is otherwise forbidden by law to inform the Client, for instance, to preserve the confidentiality of investigation by a Public Authority. GamaLearn will inform the Client if it becomes aware of any notice, inquiry, or investigation by a Supervisory Authority with respect to the processing of Client Personal Data under this DPA conducted between you and us.

5.3. Security Measures.

GamaLearn shall implement and maintain appropriate technical and organisational measures to protect Client Data from personal data breaches (the '**Security Incidents**'), in accordance with our security standards set out in the Schedule 2 of this DPA. You acknowledge that security measures are subject to technical progress so that we may modify or update the Schedule 2 of this DPA at our sole discretion provided that such modification or update does not result in a material degradation in the security measures offered by the Schedule 2 of this DPA at the time of signing this DPA.

5.4. Security Incident.

Upon becoming aware of a Security Incident, GamaLearn shall: (i) notify you without undue delay after we become aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by you; and (iii) promptly take reasonable steps to contain and investigate any Security Incident so that you can notify competent authorities and/or affected Data Subjects of the Security Incident. Our notification of or response to a Security Incident shall not be construed as an acknowledgement by us of any fault or liability regarding the Security Incident.

5.5. Confidentiality.

GamaLearn will not access or use, or disclose to any third party, any Client Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with contractual and legal obligations or binding order of a public body (such as a subpoena or court order). We shall ensure that any employee/contractor to whom we authorise access to Client Data on our behalf is subject to appropriate confidentiality contractual or statutory duty obligations with respect to Client Data, including after the end of their respective employment or termination or expiration of contract.

5.6. Return or Deletion of Client Data.

GamaLearn shall, and shall cause any Sub-processors to, at the choice of Client, return all the Client Personal Data and copies of such data to Client or securely destroy them and demonstrate to the satisfaction of Client that it has taken such measures, unless GDPR or Other Data Protection Laws and Regulations prevent GamaLearn from returning or destroying all or part of the Client Personal Data in our possession. In such a case, GamaLearn agrees to preserve the confidentiality



of the Client Personal Data retained by it and that it will only actively process such Client Personal Data after such date in order to comply with applicable laws and regulations or contractual obligations.

5.7. Reasonable Assistance.

GamaLearn agreed to provide reasonable assistance to Client regarding:

- (i) any request from a Data Subject in respect of access to or the rectification, erasure, restriction, portability, blocking or deletion of Client Personal Data that GamaLearn on behalf of Client. In the event that a Data Subject sends such a request directly to GamaLearn, Section 7 of this DPA shall apply;
- (ii) the investigation of Security Incident and communication of necessary notifications regarding such Security Incidents subject to Section 5.4 of this DPA;
- (iii) preparation of data protection impact assessments and, where necessary, consultation of Client with the Supervisory Authority under Articles 35 and 36 of the GDPR.

6. Audit and Certification

If a Supervisory Authority requires an audit of the data processing facilities from which GamaLearn processes Client Personal Data to ascertain or monitor Client's compliance with the GDPR or Other Data Protection Laws and Regulations, GamaLearn will cooperate with such audit. The Client is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time GamaLearn expends for any such audit, in addition to the rates for services performed by GamaLearn.

The Client may, prior to the commencement of processing, and at regular intervals, thereafter, audit the technical and organisational measures taken by GamaLearn. If the Client is the controller with respect to the personal data processed by GamaLearn on its behalf, upon reasonable and timely advance agreement, during regular business hours and without interruption to GamaLearn's business operations, GamaLearn may provide Client with all information necessary to demonstrate compliance with its obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client with respect to such processing.

GamaLearn shall, upon the Client's written request and within a reasonable period, provide Client with all information necessary for such audit, to the extent that such information is within GamaLearn's control and GamaLearn is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

7. Data Subject Request

In the event that a Data Subject contacts us with regard to the exercise of their rights under GDPR and Other Data Protection Laws and Regulations (in particular, requests for access to, rectification or blocking of Client Personal Data), we will use all reasonable efforts to forward such requests to you. If we are legally required to respond to such a request, we shall immediately notify you and provide you with a copy of the request unless we are legally prohibited from doing so.

8. Sub-processors and Third-party Processors

You agree that we may engage sub-processors in accordance with provisions set out in Clause 9 of respective SCCs to assist in fulfilling our obligations with respect to the provision of the services under the Terms. We agree to inform the Client of any intended changes concerning the addition or replacement of Sub-processors, thereby giving the Client the opportunity to object to such changes within the period specified in SCC.

Client acknowledges that in the provision of some services, GamaLearn, on receipt of instructions from Client, may transfer Client Personal Data to and otherwise interact with third party data



processors. Client agrees that if and to the extent such transfers occur, Client is responsible for entering into separate contractual arrangements with such third-party data processors binding them to comply with obligations in accordance with the GDPR and Other Data Protection Laws and Regulations. For the avoidance of doubt, such third party data processors are not Sub-processors in the meaning of this DPA.

9. Data Transfers

9.1. Transfers of the Client Data

Parties agree that when the processing of the Client Data on behalf of the Client in connection with Services constitutes a transfer under the GDPR and Other Data Protection Laws and Regulations and appropriate safeguards are required, such processing will be subject to the Standard Contractual Clauses are deemed to be incorporated into and form part of this DPA as further described in subsections 9.2. and 9.3. of this DPA. If and to the extent the SCCs, as applicable, conflict with any provision of the DPA, the SCCs shall prevail to the extent of such conflict.

9.2. Transfers under the GDPR

When the processing of the Client Data on behalf of a Client in connection with Services constitutes a "transfer" under the GDPR, Standard Contractual Clauses shall apply. When the Client is a controller and the Company is a processor, Module Two of the EU SCCs shall apply, and when the Client is a processor, and the Company is a sub-processor, Module Three of the EU SCCs shall apply.

For the purpose of the EU SCCs, the Company acts as a "data importer", and the Client acts as a "data exporter". The relevant provisions contained in the EU SCCs are incorporated by reference and are an integral part of this DPA. Clauses and annexes of the EU SCCs deemed to be completed as follows:

- (i) in Clause 7, the optional docking clause shall not apply;
- (ii) in Clause 9, Option 2 (General written authorization) shall apply. For the purpose of Clause 9 (a), the time period for informing the data exporter shall be 10 days;
- (iii) in Clause 11, the optional provision shall not apply;
- (iv) in Clause 13, a particular option shall apply depending on the specific case;
- (v) in Clause 17, Option 1 shall apply. The Parties agree that this shall be the law of the Republic of Estonia;
- (vi) in Clause 18(b), disputes shall be resolved by the courts of the Republic of Estonia;
- (vii) Annex I of the EU SCCs is deemed completed with the information set out in Schedule 1 of this DPA;
- (viii) Annex II of the EU SCCs is deemed completed with the information set out in Schedule 2 of this DPA.

9.3. Transfers under the Oman PDPL

When the processing of data in connection with the Services involves an international transfer subject to Oman's Personal Data Protection Law (Royal Decree No. 6/2022), such transfer shall be conducted under one of the following lawful bases: the explicit consent of the data subject to the transfer; a transfer to a jurisdiction deemed to provide an adequate level of data protection,



as assessed by the data controller; a transfer permitted under a binding international treaty or with authorization from the Ministry of Transport, Communications and Information Technology.

The data controller shall be responsible for ensuring that the conditions for the lawful international transfer of personal data are met, including verifying the legal basis for transfer, performing any required adequacy assessments, and documenting compliance with the requirements of Omani law.

9.4. Transfers under the KSA PDPL

When the processing of data involves an international transfer from the Kingdom of Saudi Arabia under the Saudi Personal Data Protection Law (PDPL), Royal Decree M/148, the following shall apply. Transfers may be carried out if the receiving country provides an adequate level of data protection, or the transfer is necessary for contract performance, public interest, or legal claims, or the transfer is based on Standard Contractual Clauses approved by the Saudi Data and AI Authority (SDAIA).

If no specific exemption is available, the Parties agree to enter into the SDAIA Standard Contractual Clauses, which are incorporated by reference into this DPA.

The Second Template of the SCCs applies when the Client is a Controller and the Company is a Processor. In this case, the transfer involves Personal Data being sent from the Controller (the data exporter) to the Processor (the data importer) outside the Kingdom.

The Third Template applies when the Client is a Processor and the Company is a Sub-Processor. The transfer involves Personal Data being sent from one Processor (the data exporter) to another Processor acting as a Sub-Processor (the data importer) outside the Kingdom.

Appendix 1 (Parties and List of Parties) and Appendix 2 (Description of the Transferred Personal Data) shall be deemed completed with the information set out in Schedule 1 of this Data Processing Agreement (DPA). Appendix 3 (Technical and Organisational Security Measures) shall be deemed completed with the information set out in Schedule 2 of this DPA.

9.5. Transfers under the UAE PDPL

When the processing of Client Data involves a transfer from the UAE subject to Federal Decree-Law No. 45 of 2021, international transfers may be made to jurisdictions recognized as providing an adequate level of protection; or with data subject consent, or pursuant to contractual clauses or other safeguards prescribed or permitted by the UAE Data Office or other relevant authority.

The data controller shall be responsible for ensuring that the conditions for the lawful international transfer of personal data are met, including verifying the legal basis for transfer, performing any required adequacy assessments, and documenting compliance with the requirements of UAE law.



SCHEDULE 1 - DESCRIPTION OF PROCESSING

A. LIST OF PARTIES

Data exporter

Name: 'You', 'Client'.

Address: the relevant information is contained in the Client's account.

Contact person's name, position and contact details: the relevant information is contained in the Client's account.

Activities relevant to the data transferred under these Clauses:

- provision of SwiftAssess services (e.g. Digital Assessments, SmartPaper, Observer, Test Center, and Immersive Assessments);

Signature and date: By entering into the Terms, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the effective date of the agreement.

Role: For the purposes of Addendum I (Controller-to-Processor transfer) Client is a controller. For the purposes of Addendum II (Processor-to-Processor transfer) Client is a processor.

Data importer

Name: GamaLearn

Address: P.O. Box: 43957, Khalifa Street, GIBCA Tower, No. 002, Abu Dhabi, United Arab Emirates

Contact person's name, position and contact details: Omar Rizk, CTO, +971 2 6222345

Activities relevant to the data transferred under these Clauses:

- provision of SwiftAssess services (e.g. Digital Assessments, SmartPaper, Observer, Test Center, and Immersive Assessments);

Signature and date: By entering into the Terms, data importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the effective date of the agreement.

Role: processor

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred:

- Clients' students, employees, or other third parties whose personal information is processed when Clients use SwiftAssess services.

2. Categories of personal data transferred:

- Any relevant personal data of the Client's students, employees, or other third parties whose personal information is processed when Clients use SwiftAssess services.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:

The transferred data may include special categories of personal data (sensitive data). The restrictions and safeguards specified in Annex II apply to these categories of personal data (if any).

4. The frequency of the transfer:

Personal data is transferred on a continuous basis.

5. Nature of the processing:

Personal data processing consists of the following:



- provision of SwiftAssess services (e.g. Digital Assessments, SmartPaper, Observer, Test Center, and Immersive Assessments);

6. Purpose(s) of the data transfer and further processing:

The purpose of the data processing under these Clauses is the performance of the services for data exporter by the data importer under the service agreement concluded between the data importer and the data exporter including but not limited to the provision of SwiftAssess services.

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The personal data shall be stored for the duration of these Clauses concluded between the data importer and the data exporter, unless otherwise agreed in writing or the data importer is required by applicable law to retain some or all of the transferred personal data.

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

subject matter: the performance of services

nature: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, alignment or combination, restriction, erasure or destruction.

duration: the performance of the services for data importer by the (sub-) processor under the service agreement concluded between the data importer and (sub-) processor.

C. COMPETENT SUPERVISORY AUTHORITY

In accordance with Clause 13, competent supervisory authority under these Clauses is determined depending on what version of Clause 13(a) applies to the data exporter.



SCHEDULE 2 - TECHNICAL AND ORGANISATIONAL MEASURES

Description of the technical and organisational measures implemented by the data importer(s) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

- Data importer uses reliable service providers and monitors what technical and organisational measures they have in place to ensure that data is protected at all times.
- Data importer is committed to preserving the confidentiality, integrity, availability and resilience of all the personal data in question throughout the data importer processing activities and ensuring that personal data are protected against loss and destruction by implementing appropriate internal information security policies and procedures.
- To ensure the security and protection of personal data, the data importer uses a backup system as part of its data management practices.
- Data importer has adopted data encryption policies that are designed to protect the privacy of data subjects by ensuring the security of personal data processing.
- All servers and workstations of the data importer have proper security configurations and are continuously checked for vulnerabilities. Any vulnerabilities identified are addressed accordingly.
- Data importer has implemented measures designed to ensure that personal data, in the event of a physical or technical incident, may be restored in a timely manner.
- Data importer has implemented comprehensive measures designed to prevent unauthorised access for processing of personal data and prevent the use of automated processing systems by unauthorised persons. The data processing systems can only be used if the users have previously undergone strong identification and authentication controls. All services and workstations require a password that complies with the respective password policy. The personal data is subject to a strictly need-to-know principle of access and can be displayed to the authorised staff members and users only.
- Data importer has implemented measures designed to prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data. Software solutions installed allow to trace whether and by whom personal data have been entered into the data processing systems and whether and by whom personal data have been changed or deleted.
- The data importer has taken a number of steps to ensure physical security at locations where personal data is processed (e.g., using only data importer equipment when necessary, locking access to equipment when not in use, access to facilities is strictly regulated, etc.).
- Data importer's staff shall comply with Data importer's internal policies, procedures and other applicable documents. It is required to read the current version of such documents to any staff member before undertaking any of their responsibilities regarding personal data processing. All staff members shall receive appropriate security training or instructions concerning processing of personal data.
- Data importer has adopted information security policies, procedures and other documents for ensuring the fulfillment of data minimization, data quality, limited data retention and accountability principles and ensuring system configuration.



- The data importer shall implement technical and organizational measures that meet the requirements of the UAE PDPL, KSA PDPL, and Oman PDPL, including encryption, access controls, data minimization, breach detection, role-based access, and secure destruction procedures.

Technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

- The transfer of personal data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If personal data is transferred to companies located outside the EEA, the data exporter provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the EU SCCs.

DRAFT VERSION



SCHEDULE 3 - LIST OF SUB-PROCESSORS

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Sub-processor 1:

Name: DigitalOcean LLC.

Address: 101 6th Ave New York, NY 10013, USA

Contact person's name, position and contact details: <https://docs.digitalocean.com/support/>

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): to use as a hosting infrastructure for our Site, Community, and website <https://gamalearn.com>.

Sub-processor 2:

Name: Microsoft Azure (Microsoft Corporation)

Address: One Microsoft Way, Redmond, WA 98052, USA

Contact person's name, position and contact details: <https://azure.microsoft.com/en-us/support/>

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): to use as a hosting infrastructure for our Application.

Sub-processor 3:

Name: WordPress (Automattic Inc.)

Address: 60 29th Street #343, San Francisco, CA 94110, USA

Contact person's name, position and contact details: <https://automattic.com/contact/>

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): to build websites on our Platform.

