Data Processing Addendum

Revised February 1, 2023

This Data Processing Addendum (the “DPA”) is an agreement between Sales Impact Academy, Inc. (“SIA” or “we”) and you, the Customer (“you” or “Customer”), collectively referred to as the Parties and individually as a Party. This DPA supplements the underlying agreement between the Parties (the “Customer Agreement”) and governs the Customer’s usage of SIA Services.

In this connection, SIA processes personal data on behalf of the Customer. You enter into this DPA when you enter into the Customer Agreement and this DPA is incorporated in and forms part of the Customer Agreement between SIA and you.

1. Definitions

1.1. In this DPA, the following terms have the following meanings:

“Affiliate” means an entity that directly or indirectly controls, or is controlled by, or under common control with, another entity. “Control” for the purposes of this definition means the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the general management of the company;

"Applicable Data Protection Law" shall mean (i) Regulation 2016/679 of the European Parliament and of the Council, the General Data Protection Regulation (“GDPR”) on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, (ii) the GDPR as it forms part of UK law by virtue of Section 3 (10) of section 3(10) of the DPA 2018, as supplemented by section 205(4) ("UK GDPR"),and (iii) any other applicable law or regulation which governs the Processing of Personal Data and the free movement of such data.

“CCPA” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

“Controller", "Processor", "Data Subject”, "Personal Data" "Processing" and "Process" shall have the meanings given in Applicable Data Protection Law.

“Customer Data” means all data, including all text, sound, video, or image files related to the Customer that are provided to SIA by Customer through use of the Services. Customer Data also includes Customer’s Personal Data that is Customer Data.

"DPA 2018" means the Data Protection Act 2018 in the UK.

"DP Regulator" means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws.

"EEA" means the European Economic Area.

"SCCs**"** means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data in countries not otherwise recognised as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

“IDTA” means the International Data Transfer Addendum set out in Addendum II of this DPA. "Model Clauses" means the EU SCCs and/or the UK SCCs for Processors.

“Services” means the services provided by SIA as described in the Customer Agreement.

“User” means an individual who is authorised to use the Service (for instance individuals who have been supplied with a user identification and password by the Customer). Users may include Customer’s or a Customer Affiliate’s employees, consultants, contractors, agents or other third parties.

2. Description of Personal Data Processed; Instructions for Processing

2.1. In performing the obligations under the Customer Agreement and this DPA, SIA will Process the Personal Data on behalf of the Customer in accordance with Applicable Data Protection Laws. In this context and for the purposes of the Applicable Data Protection Laws, Customer is the data Controller and SIA is the data Processor; and for the purposes of the CCPA (to the extent applicable), Customer is the Business and SIA is the Service Provider.

2.2. SIA shall process Customer's Personal Data as part of providing Customer with the Services, pursuant to the specifications and for the duration under the Customer Agreement.

2.3. Customer shall, in its use of the Services, only submit or otherwise have Personal Data processed in accordance with the requirements of Applicable Data Protection Laws. SIA will only process Personal Data on behalf of and in accordance with Customer’s reasonable instructions. Customer instructs SIA to process Personal Data for the following purposes: (i) processing related to the Services in accordance with the Customer Agreement; (ii) processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the Customer Agreement; (iii) rendering Personal Data fully and irrevocably anonymous and non-personal, in accordance with applicable standards recognized by Applicable Data Protection Laws and guidance issued thereunder; and (iv) processing as required under any applicable laws to which SIA is subject, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that SIA shall inform Customer of the legal requirement before processing, unless prohibited under such law or requirement.

2.4. To the extent that SIA cannot comply with an instruction from Customer, (i) SIA shall promptly inform Customer, providing relevant details of the problem, (ii) SIA may, without any kind of liability to Customer, temporarily cease all processing of the affected Personal Data (other than securely storing such data) and/or suspend access to the Customer’s account, and (iii) if the parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Customer Agreement and this DPA with respect to the affected processing. Customer will have no further claims against SIA (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Customer Agreement and the DPA as described in this paragraph.

2.5. CCPA Standard of Care; No Sale of Personal Information. SIA acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that SIA provides to Customer under the Agreement. SIA shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Customer's behalf, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as stipulated in the Customer Agreement and this DPA. SIA certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Personal Information Processed hereunder, without Customer's prior written consent, nor taking any action that would cause any transfer of Personal Information to or from SIA under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA. For the avoidance of doubt, SIA will not use, retain or disclose Personal Information for any purpose other than providing the Service.

3. SIA Obligations

3.1. SIA represents and warrants that it will process Personal Data only on the documented instructions and for the purposes incorporated in this DPA and the Customer Agreement (the "Permitted Purpose"), unless required to do so by EU or Member State law to which SIA is subject.

3.2. To the extent that SIA does not comply with the instructions of Customer and independently makes determinations about the means and purposes of the processing, SIA acknowledges that it will be considered to be a Controller (as defined in the Applicable Data Protection Law) in respect of that processing activity.

3.3. In addition to the confidentiality provisions of the Customer Agreement (if applicable), SIA will ensure that SIA's employees, subcontractors or other authorized personnel ("Authorised Persons") that process Personal Data are subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Personal Data who is not under such a duty of confidentiality. SIA shall ensure that all Authorized Persons process the Personal Data only as necessary for the Permitted Purpose and SIA shall be fully liable for the actions of such Authorised Persons.

4. Customer Obligations

4.1. Customer shall:

(a) comply with; and

(b) procure the compliance of Customer Affiliates, Users, other contacts of the Customer or Customer Affiliates, or third parties who may use the Services, with the Applicable Data Protection Laws in Processing Personal Data in relation to the Services.

4.2 In particular, the Customer shall:

(a) as required by the Applicable Data Protection Laws, obtain any necessary consents and provide sufficient information to Data Subjects regarding the Processing of their Personal Data, or procure the same, for:

(i) the Customer to disclose the Personal Data to SIA; and

(ii) SIA to Process the Personal Data for the purposes set out in the Customer Agreement and in accordance with the Applicable Data Protection Laws;

(b) ensure that the Customer's instructions to SIA for Processing Personal Data as the Customer's Processor (where relevant) comply with the Applicable Data Protection Laws and

do not put SIA in breach of the Applicable Data Protection Laws or violate the rights of any Data Subject; and

(c) provide reasonable assistance to SIA in complying with SIA's obligations under the Applicable Data Protection Laws, including by entering into any amendments or additions to this DPA which may be necessary to reflect any changes in the Customer's, or SIA's, Personal Data Processing activities, or otherwise as required by the Applicable Data Protection Laws.

4.3 Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Without limitation, Customer will provide all necessary notices to relevant Data Subjects, including a description of the Services, and secure all necessary permissions and consents, or other applicable lawful grounds for processing Personal Data pursuant to this DPA. SIA will inform Customer if, in SIA's opinion, an instruction infringes any provision under any Applicable Data Protection Laws and will be under no obligation to follow such instruction, until the matter is resolved in good-faith between the parties.

5. Sub-Processors

5.1. SIA may hire Sub-processors to provide certain limited or ancillary services on its behalf. Customer authorizes SIA's engagement of Sub-processors. Where the Controller to Processor SCCs apply, the Parties agree to use "Option 2" in clause 9 of the Controller to Processor SCCs (i.e., Customer's general written authorization for the engagement of SIA's Sub-processors). SIA makes available information about Sub-processors on SIA's website https://www.salesimpact.io/privacy-policy/

5.2. From time to time, SIA may engage new Sub-processors to process personal data on Customer's behalf. SIA will give the Customer notice (by updating the website or providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor in advance of engaging that new Sub-processor. Customer may object to the processing of Customer's Personal Data by the new Sub-processor, on reasonable and explained grounds, by providing a written objection to legal@salesimpact.io within 5 business days following SIA's notice to Customer of the intended engagement with the new Sub-Processor. If Customer timely sends SIA a written objection notice, the parties will use good-faith efforts to resolve Customer's objection. In the absence of a resolution, SIA will use commercially reasonable efforts to provide Customer with the same level of service without using the new Sub-processor to process Customer's Personal Data.

5.3. In the event that SIA engages a Sub-Processor to assist with or carry the processing activity on its behalf, SIA represents and warrants that the processing activity is carried out with at least the same level of protection for the Personal Data and the rights of Data Subjects as required in the Customer Agreement and this DPA and that at a minimum the same data protection, security, and confidentiality obligations and as set out in this DPA and Customer Agreement shall be imposed on the Sub-Processor. Where the Sub-Processor fails to fulfil its data protection obligations, SIA shall remain fully liable to Customer for the performance of the Sub-Processor's obligations.

6. Technical and Organizational Measures

6.1. SIA represents and warrants that SIA has implemented, and will maintain for the duration in which SIA holds Customer Personal Data, all appropriate technical and organizational measures to ensure a level of security required to protect Personal Data from any actual loss, unauthorized or unlawful processing, destruction, damage, alteration or accidental or unlawful destruction, loss, alteration,

unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed as further described in Appendix A.

6.2. SIA regularly monitors its compliance with these measures. SIA will not materially decrease the overall security of the Services during the term of the Customer Agreement.

7. International transfers

7.1. SIA will at all times provide an adequate level of protection for the Personal Data, wherever processed, in accordance with the requirements of Applicable Data Protection Law.

7.2. For the purpose of this DPA and compliance with the GDPR, SIA and the Customer agree to enter into the Standard Contractual Clauses issued by the EU Commission on June 4, 2021. Where applicable, and as set out in Addendum I, for transfers of Personal Data from a Customer established in the EEA or Switzerland, as a data controller, to an SIA entity established in a country outside the EEA, or Switzerland as a data processor, the Parties agree to enter into the Controller to Processor SCCs. The Controller to Processor SCCs will only apply to Personal Data that is transferred outside the EEA or Switzerland, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data.

7.3. For purposes of this DPA and compliance with the UK GDPR, the Parties agree to enter into the IDTA issued by the UK Information Commissioner's Office on March 21, 2022, as set out in Addendum II. The IDTA will only apply to Personal Data that is transferred outside the UK, either directly or via onward transfer, to any country not recognized by the UK as providing an adequate level of protection for personal data.

7.4. In the event of any conflict or inconsistency between the DPA and any other terms in the Customer Agreements, the DPA shall prevail. The provisions of the DPA supersede any conflicting provisions of SIA Privacy Notice that otherwise may apply to processing of Customer Data. Where the SCCs and/or IDTA apply and as required by Clause 5 of the Controller to Processor SCCs and Clauses 9 thru 11 of the IDTA, the Controller to Processor SCCs and IDTA prevail over any other term of the DPA Terms and terms of the Agreement.

If SIA is processing Personal Data within the scope of the CCPA, SIA makes the following additional commitments to Customer. SIA will process Customer Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will SIA sell any such data. These CCPA terms do not limit or reduce any data protection commitments SIA makes to Customer in the DPA or Customer Agreement.

7.5. SIA acknowledges that Customer may disclose this DPA and any relevant privacy provisions in the Customer Agreement(s) to the US Department of Commerce, the Federal Trade Commission, European data protection authority, or any other US or EU judicial or regulatory body upon their request subject to prior notice to the Customer, when reasonably possible.

8. Notification

8.1. SIA has in place reasonable and appropriate security incident management policies and procedures and will notify Customer without undue delay (and in any event within 48 hours) after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed (a "Personal Data Breach").

8.2. SIA will immediately inform Customer:

(a) if an instruction infringes the GDPR or other EU or Member State data protection provisions;
(b) of any event or incident which puts the Personal Data at risk; or
(c) any legally binding request for disclosure of the Personal Data by a law enforcement or regulatory authority.

8.3 SIA shall make reasonable efforts to identify the cause of such Personal Data Breach, and take those steps as SIA deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach, to the extent that the remediation is within SIA's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Customer or Customer's Users.

9. Deletion and Return of Personal Data

9.1. Upon request by Customer, or after completion of the processing of data pursuant to the Customer Agreement or this DPA, SIA will, at Customer's option, delete or return all Personal Data to Customer (including any Personal Data subcontracted to a third party for processing). This requirement shall not apply to the extent that SIA is required by any EU (or any EU member state) law to retain some or all of the Personal Data, in which event SIA shall isolate and protect that Personal Data from any further processing except to the extent required by such law.

10. Information Requests and Audit Rights

10.1. SIA agrees to keep records of all categories of processing activities and to make available all information reasonably necessary to demonstrate compliance with the obligations laid out in this DPA and the relevant provisions of the GDPR, and cooperate with and contribute to audits and inspections, whether by Customer, its auditors or an EU regulatory body.

10.2. SIA agrees to cooperate with Customer to provide all reasonable and timely assistance to Customer to enable Customer to:

(a) comply with any obligations under Applicable Data Protection Law including in particular those set out in Articles 32 to 36 of the General Data Protection Regulation;
(b) conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority;
(c) respond to any request from a Data Subject to exercise rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable) and SIA agrees to promptly inform Customer if such a request is received directly; and
(d) respond to and comply with any investigations, complaints or requests for information by a Data Subject or person or regulatory, supervisory, or governmental authority in connection with the processing of the Personal Data.

10.3. SIA conducts audits, inspections or questionnaires to ensure it is processing Personal Data in compliance with Applicable Data Protection Law, and this DPA. Such audits occur once during a twelve (12) month period, unless Customer is required to conduct an additional audit by a relevant Data Protection Authority, or Customer reasonably believes that an additional audit is required due to a data breach or to protect Customer's Personal Data.

10.4. Customer can request a questionnaire or security report for the purpose of reviewing the specific physical, technical, administrative and organizational security measures in place relating to all Personal Data being processed or stored by SIA on behalf of Customer, pursuant to the Customer Agreement and this DPA. Customer agrees to make these requests with reasonable notice, during SIA's normal business hours, and in a manner which will limit interference with SIA's normal business operations.

11. Liability

11.1. The parties' liability in the aggregate arising out of or in relation to this DPA, whether in contract, tort (including negligence), misrepresentation, or otherwise, shall be subject to any limitation of liability provisions in the Customer Agreement, and, only for the purposes of this DPA, any reference to the liability of a party in those Customer Agreement provisions shall be taken to mean to the liability of that party and its Affiliate.

12. General

12.1. Except as specifically set forth in this DPA, all of the terms and provisions of the Customer Agreement shall remain unmodified and in full force and effect. In the event of any conflict between the Customer Agreement and this DPA, the terms of this DPA will prevail.

APPENDIX A: SECURITY MEASURES

("Platform" – https://www.salesimpact.io)

SIA has implemented and will maintain for Customer Data the following security measures, which in conjunction with the security commitments in this DPA, are SIA's only responsibility with respect to the security of that data.

SPECIFIC TECHNICAL AND ORGANISATIONAL SECURITY SAFEGUARDS:

1. The following specific safeguards are made for SIA's physical security:

a) Access control to physical facilities,
b) Password-protection of physical equipment and outsourced systems (including databases) by suitably strong passwords, specifically, passwords no less than 8 characters and of at least alphanumerical symbol variance,
c) Only authenticated, encrypted traffic for administrative access to systems (including databases),
d) Data center redundancy of all critical infrastructure, eliminating physical risks to equipment such as fire, power failure, or similar,
e) Periodical monitoring for known vulnerabilities and established process(es) for addressing such vulnerabilities without undue delay.

2. The following specific safeguards are made for SIA's technical security:

a) at an application-level, the Platform requires authentication via user / password combination and has a fine-grained access and authorization engine for controlling resource access,
b) on a network communication level, any communication with the Platform is encrypted, as is application-database traffic,
c) as for data storage, the Platform uses state of the art data centers for storage of database data and documents, which means that data is safe, encrypted at rest, backed up, and roll-backable in case of incidents,
d) data center redundancy, backups (including at least daily backups of Customer's data), deployment and rollout methods and contingency plans enable suitable and timely recovery of the entire Platform (in case of a major incident),
e) all Platform activity (including database activity) is logged for accountability,
f) SIA's internal data networks are secured by expert third parties.

3. The following specific safeguards are made for SIA's organizational security:

a) All relevant SIA employees are briefed regularly on the Processor's security matters and how to respond to security incidents,
b) All SIA's employees follow SIA's internal Employee Code of Conduct, which spells out relevant best practice employee security behavior, such as keeping passwords personal, strong and secret.
c) SIA undertakes regular security reviews to secure a constantly sufficient level of security and develops and implements its business using the principles of privacy by design and privacy by default.

4. The following specific safeguards are made for SIA's deletion of personal data:

a) SIA keeps a digital record of what personal data is stored where on behalf the Controller, so when deleting data is mandated, SIA knows which data to delete,
b) SIA maintains a standard procedure to delete such data,
c) SIA has procedures to identify personal data that must be deleted due to age.

5. SIA shall ensure that Sub-Processors will implement the appropriate technical and organizational measures in such a way that the processing meets the requirements of the Applicable Data Protection Law.

APPENDIX B – DATA SUBJECTS AND CATEGORIES OF PERSONAL DATA

1. CATEGORIES OF PERSONAL DATA

1.1 The categories of personal data considered in the context of this DPA:

a) General Personal Data, including any data about an identified or identifiable data subject, except for those mentioned in points b) and c). Examples of such data include, but are not limited to, first name, middle names, last name, title, emails, phone numbers, addresses, IP-addresses, un-hashed cookies, other personal identifiers, birthday.

b) Sensitive Personal Data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sex life or sexual orientation, genetic data and biometric data.

c) Other Personal Data, relating to criminal offences and serious social problems.

2. CATEGORIES OF PERSONAL DATA PROCESSED

According to the Customer's instructions, SIA will process General Personal Data (see 1.1.a above) provided by the Customer. SIA does not process Sensitive Personal Data or Other Personal Data as described in 1.1.b and 1.1.c above.

3. CATEGORIES OF DATA SUBJECTS PROCESSED

3.1 According to the Customer's instructions, SIA may process personal data for the Customer concerning the following categories of data subjects in connection with the services:

a) employees, contractors and temporary workers (current, former, prospective) of data exporter, or
b) data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former).

ADDENDUM 1– STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR) MODULE II

1. Where the ex-EEA Transfer is a Controller to Processor transfer, specifically where Customer acts as the Controller and data exporter, and SIA acts as Customer's Data Processor and data importer, only the provisions relating to Module II apply to such ex-EEA Transfer.

2. The parties agree that the terms of the EU SCCs as amended below are hereby incorporated by reference and shall apply to an ex-EEA Transfer as follows:
    a. Clause 7 (Docking Clause) shall not apply.
    b. Option 2: General Written Authorisation applies and the minimum time period for the data importer to specifically inform the data exporter in writing of any intended changes to that list in accordance with Clause 9 shall be thirty (30) days;
    c. In Clause 11 of the EU SCCs, the optional language will not apply.
    d. In Clause 17 of the EU SCCs, Option 1 shall apply, and the Parties agree that the EU SCCs shall be governed by the laws of the Republic of Ireland.
    e. In Clause 18(b) of the EU SCCs, disputes will be resolved before the courts of the Republic of Ireland.
    f. To the extent there is any conflict between the EU SCCs and any other terms in this DPA or the Agreement, the provisions of the EU SCCs will prevail.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s):
Name: …The Customer, as defined in the SIA Terms and Conditions (on behalf of itself and its Permitted Affiliates)

Address: …The Customer's address as set out in the Order Form

Contact person's name, position and contact details: … The Customer's contact details, as set out in the Order Form

Activities relevant to the data transferred under these Clauses: … Processing of Personal Data in connection with Customer's use of the SIA Services under the SIA Terms and Conditions

Role (controller/processor): …Controller
…
Data importer(s):

Name: …Sales Impact Academy, Inc.

Address: …

Contact person's name, position and contact details: …General Counsel legal@salesimpact.io

Activities relevant to the data transferred under these Clauses: … Processing of Personal Data in connection with Customer's use of the SIA Services under the SIA Terms and Conditions.

Role (controller/processor): …Processor

B. DECRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Customer may submit Personal Data in the course of using the Services, the extent of which is determined and controlled by Customer in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Customer contacts and other end users including its employees, contractors, collaborators and subcontractors.

Categories of personal data transferred

The personal data that is provided to SIA and included in email, documents and other data in electronic form in the context of the Services. SIA acknowledges that, depending on Customer's use of the Services, Customer may elect to include personal data from any of the following categories in the personal data:

General Personal Data, including any data about an identified or identifiable data subject, except for those mentioned in points b) and c). Examples of such data include, but are not limited to, first name, middle names, last name, title, emails, phone numbers, addresses, IP-addresses, un-hashed cookies, other personal identifiers, birthday, sex.

Authentication data (for example user name/handle, password, security question, audit trail);
Contact information (for example physical addresses, email, phone numbers, social media identifiers);
Financial information (for example bank account name and number, credit card name and number, and invoice number;
Photos, video and audio;
Internet activity (for example browsing and search history while on the Platform);

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
… Not applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
… On a continuous basis as necessary for the data importer to meet its obligations in conjunction with the provision of the Services for the term of the agreements with the data exporter.

Nature of the processing
…The nature and purpose of the processing shall include the collection, organization, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the personal data as necessary to provide the products or services pursuant to the agreements with data exporter.

Purpose(s) of the data transfer and further processing
…Personal data will be processed in conjunction with data exporter's Customer Agreement to allow the data importer to fulfill its obligations thereunder.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
…Personal data will be retained for so long as the user(s) continue to maintain and use their accounts. Dormant accounts are checked intermittently and where contact cannot be made with the user to confirm their intent to maintain the account, the account is canceled. Upon such cancelation all date associated with that account will no longer be identifiable to a natural person.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
…Sub-processors are retained in support of the SaaS products/services provided to data exporters and are contractually bound as to subject matter, nature and duration of the processing similarly in kind as the data importer taking into account the sub-processors specific role.

C. COMPETENT SUPERVISORY AUTHORITY
Identification of the competent supervisory authority/ies in accordance with Clause 13

If the data exporter is established in an EU Member State*: the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer will act as competent supervisory authority.*

If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR)*: the supervisory authority of the Member State in which the representative is established will act as competent supervisory authority.*

If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU*: the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the Standard Contractual Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, will act as competent supervisory authority.*

ANNEX II - SECURITY MEASURES

("Platform" – https://www.salesimpact.io)

SIA has implemented and will maintain for Customer Data the following security measures, which in conjunction with the security commitments in this DPA, are SIA's only responsibility with respect to the security of that data.

SPECIFIC TECHNICAL AND ORGANISATIONAL SECURITY SAFEGUARDS:

1. The following specific safeguards are made for SIA's physical security:

a) Access control to physical facilities,
b) Password-protection of physical equipment and outsourced systems (including databases) by suitably strong passwords, specifically, passwords no less than 8 characters and of at least alphanumerical symbol variance,
c) Only authenticated, encrypted traffic for administrative access to systems (including databases),
d) Data center redundancy of all critical infrastructure, eliminating physical risks to equipment such as fire, power failure, or similar,
e) Periodical monitoring for known vulnerabilities, e.g. scans against OWASP top 10, and established process(es) for addressing such vulnerabilities without undue delay.

2. The following specific safeguards are made for SIA's technical security:

a) at an application-level, the Platform requires authentication via user / password combination and has a fine-grained access and authorization engine for controlling resource access,
b) on a network communication level, any communication with the Platform is encrypted, as is application-database traffic,
c) as for data storage, the Platform uses state of the art data centres for storage of database data and documents, which means that data is safe, encrypted at rest, backed up, and roll-backable in case of incidents,
d) data center redundancy, backups (including at least daily backups of Customer's data), deployment and rollout methods and contingency plans enable suitable and timely recovery of the entire Platform (in case of a major incident),
e) all Platform activity (including database activity) is logged for accountability,
f) SIA's internal data networks are secured by expert third parties.

3. The following specific safeguards are made for SIA's organizational security:

a) All relevant SIA employees are briefed regularly on the Processor's security matters and how to respond to security incidents,
b) All SIA's employees follow SIA's internal Employee Code of Conduct, which spells out relevant best practice employee security behavior, such as keeping passwords personal, strong and secret.
c) SIA undertakes regular security reviews to secure a constantly sufficient level of security and develops and implements its business using the principles of privacy by design and privacy by default.

4. The following specific safeguards are made for SIA's deletion of personal data:

a) SIA keeps a digital record of what personal data is stored where on behalf the Controller, so when deleting data is mandated, SIA knows which data to delete,
b) SIA maintains a standard procedure to delete such data,
c) SIA has procedures to identify personal data that must be deleted due to age.

5. SIA shall ensure that Sub-Processors will implement the appropriate technical and organizational measures in such a way that the processing meets the requirements of the Applicable Data Protection Law.

ANNEX III – SUB-PROCESSORS

To help SIA deliver the Services, we engage Sub-Processors to assist with our data processing activities. A list of our Sub-Processors and our purpose for engaging them is available at https://www.salesimpact.io/privacy-policy/, which is incorporated into this DPA.

ADDENDUM II - International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The Start Date for this Addendum shall coincide with the start date of each Customer Agreement between the Parties.	
The Parties	**Exporter (who sends the Restricted Transfer)** The Exporter is the Customer as identified in the Order Form between SIA and the Customer	**Importer (who receives the Restricted Transfer)** The Importer is Sales Impact Academy Inc.
Parties' details	Exporters' details are as set forth in the Order Form.	Importer's details are as set forth in the Order Form.
Key Contact	Exporter's details are as set forth in the Order Form.	Importer's details are as set forth in the Order Form.
Signature (if required for the purposes of Section 2)	The Parties agree that their signatures affixed to the Order Form shall serve to legally bind the Parties to this Addendum.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): 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 General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No					
2	Yes	No	No	Yes	30 Business Days	
3	No					
4	No					

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: Parties are as set forth in Annex I.A of the EU SCCs found in Addendum I to the DPA.
Annex 1B: Description of Transfer: is as set forth in Annex I.B. of the EU SCCs found in Addendum I to the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Technical and organisational measures are as set forth in Annex II to the EU SCCs found in Addendum I to the DPA.
Annex III: List of Sub processors (Modules 2 and 3 only): Sub-processors are as set forth in Appendix III of the DPA

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. Clause 18 will apply in the event the Approved Addendum changes in accordance therewith

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, 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.

Interpretation of this Addendum

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. In addition, the following terms have the following meanings:

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.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils 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 applies.

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.

Hierarchy

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 Addendum 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.

Incorporation of and changes to the 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 1212, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) 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.

Amendments to this Addendum

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.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.