This Personal Data Processing Agreement ("DPA"), including the applicable Appendices, is entered into by the customer as named in the master services agreement ("the MSA") entered into between the parties ("Customer") and Teach n Go Ireland Limited ("TnG"), (each a "Party" and, together, the "Parties") and is attached to and incorporated into the MSA between Customer and TnG. The DPA, including the applicable Appendices, is effective as to each Party on the effective date of the MSA.

1. Definitions

All capitalized terms not defined herein shall have the meaning set forth in the MSA.

"Data Subject" means the subject of Personal Data.

"Data Subject Request" means a request by a Data Subject to exercise rights granted under the applicable data protection law.

"Personal Data" means any information received by TnG from, or created or received by TnG on behalf of, Customer, relating to an identified or identifiable natural person. An "identifiable natural person" is one who can be identified, directly or indirectly, in particular, by reference to an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the natural person.

"Process", "Processes" or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, including the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, transfer, dissemination by means of transmission, distribution or otherwise making available, merging, linking as well as blocking, erasure or destruction.

"Supervisory Authority" refers to the relevant government entity that is tasked with governing the Processing of Personal Data.

"Transfer" means physical or electronic movement of Personal Data from one country to another. Data transfer includes remote access to Personal Data by a user in the destination country.

2. General Provisions

2.1 This DPA applies exclusively to Personal Data Processed by TnG on behalf of Customer to fulfill TnG's obligations to provide the services via the Hosted Services in compliance with the MSA.

2.2 The Parties agree that, with respect to the Personal Data and between the Parties, Customer is the data controller, and TnG is the data processor, under applicable data protection law.

2.3 TnG shall Process Personal Data only in accordance with (i) Customer's reasonable and lawful instructions, or (ii) as required by applicable law. The Parties agree that Customer's instructions are reflected in the underlying MSA between the Parties and Appendix A, which describes the nature and purpose of the Processing, the type of Personal Data, and the Categories of Data Subjects.

3. TnG Responsibilities

3.1 Data Security. TnG shall maintain a privacy and security program that includes reasonable and appropriate measures — including technical, physical, and organizational safeguards taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons — to protect against reasonably foreseeable risks to the security, confidentiality, integrity and resilience of Personal Data, which risks could result in the unauthorized disclosure, use, alteration, destruction or other compromise of the Personal Data, including a Personal Data breach, as breach is defined under applicable data protection law.

3.2 Data Subject Requests: To the extent Customer does not have the ability to address a Data Subject Request (including via the services pursuant to the MSA), TnG shall provide reasonable assistance to facilitate the Data Subject Request, provided that Customer shall pay TnG's reasonable charges for providing such assistance on its prevailing hourly rates, and that Customer provides written instructions to TnG. Upon receipt of Customer's written instructions, TnG will take such action reasonably requested by Customer to assist Customer in responding to a Data Subject Request. In the event a Data Subject submits a Data Subject Request directly to TnG, TnG will notify Customer of the Data Subject Request and will await instructions from Customer regarding its response to the Data Subject Request.

3.3 Sub-Processors: TnG will obtain reasonable assurances, in writing, from any sub-processor that Processes Personal Data on TnG's behalf that the sub-processor will comply with the restrictions and conditions on Processing Personal Data substantially no less protective than the restrictions and conditions that this DPA imposes on TnG.

3.4 Return Or Destruction Of Personal Data: Within sixty (60) business days of the termination of the MSA, TnG will use its reasonable endeavours to return, destroy, or transfer to a third party designated by an authorized Customer representative in writing, all Personal Data. If Customer directs TnG to destroy the Personal Data, TnG will do so in a manner reasonably intended to ensure that recovery of the Personal Data would be impracticable.

4. Customer Responsibilities

4.1 Compliance. Customer shall ensure its instructions to TnG comply with applicable law. TnG is not responsible for assessing or determining for Customer if Customer's instructions are legally compliant.

4.2 Steps Prior to Transfer. Customer warrants and represents that it has taken all steps legally required under applicable law, including but not limited to, providing notice and obtaining all necessary authorizations required, prior to disclosing, transferring, or otherwise making available, any Personal Data to TnG under the MSA.

4.3 Accuracy. Customer warrants and represents that it has made reasonable efforts to ensure that any Personal Data that it discloses, transfers, or otherwise makes available to TnG under the MSA is accurate and complete.

5. Country or Regional Specific Terms

5.1 Certain jurisdictions require the Parties to include additional contractual terms. Such jurisdiction-specific terms are contained in the following appendices and are incorporated

by reference herein. Appendix A contains a general description of the transfer and is incorporated by reference in certain jurisdiction-specific appendices. The appendices are binding on the Parties as follows:

(a) **Appendix B (EU/EEA & Switzerland):** applies when (1) Customer is located in the European Economic Area ("EEA") or Switzerland, or (ii) contracting on behalf of an affiliated company(ies) located in the EEA or Switzerland, and (2) the TnG entities providing the services are located in a country that the European Union ("EU") Supervisory Authority, or Swiss Supervisory Authority, has not deemed to provide adequate data protection.

(b) **Appendix C (UK)**: applies when (1) Customer is (i) located in the United Kingdom ("UK") or is (ii) contracting on behalf of an affiliated company(ies) located in the UK and (2) the TnG entity(ies) that will be providing services is located outside of the EEA, UK, or Switzerland.

(c) **Appendix D (Intra-Europe)**: applies when (1) Customer (i) is located in the EEA, UK, or Switzerland, or (ii) is contracting on behalf of an affiliated company(ies) located in the EEA, UK, or Switzerland, and (iii) has contracted with an TnG entity located in the EEA, UK, or Switzerland, and (2) the Personal Data will not be transferred outside of the EEA, Switzerland or the UK.

(d) **Appendix E (California, USA)**: applies when Customer and the Personal Data is subject to the California Privacy Rights Act ("CPRA").

5.2 In the event of any conflict between the terms of this DPA and the terms of an Appendix regarding Personal Data subject to that Appendix, the terms of the Appendix shall prevail.

6. Miscellaneous

6.1 Survival. TnG's obligations and duties under this DPA with respect to Personal Data Processed on Customer's behalf will survive the termination of the MSA and of this DPA and will continue for as long as the Personal Data remains in TnG's possession.

6.2 Entire Agreement. This DPA contains the entire understanding of the Parties with respect to the subject matter of this DPA.

6.3 Conflicting Terms. This DPA is without prejudice to the rights and obligations of the parties under the MSA which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the MSA, the terms of this DPA shall prevail to the extent that the term at issue concerns the Processing of Personal Data.

6.4 Data Breach Notifications. If Customer determines that a data breach with respect to its Personal Data requires notification to any Supervisory Authority, Data Subjects,

and/or the public or portions of the public, Customer will notify TnG before delivering the notification and supply TnG with copies of the proposed notification that references TnG, its security measures, and/or role in the data breach, whether or not by name. Subject to Customer's compliance with applicable data protection law, Customer will consult with TnG in good faith and take account of any clarifications or corrections TnG reasonably requests to such notifications. The Parties acknowledge that it is the obligation of the Customer to determine if such breach is notifiable with reference to applicable law.

6.5 Liability. To the extent allowed by law and subject to specific terms in applicable Appendices, TnG's liability to Customer, and to each member of Customer Group (taken together), under or in connection with this DPA, including under the Appendices to this DPA, shall in no event exceed 6 month's worth of fees paid by Customer to TnG for provision of the Services.

6.6 Third-Party Rights. No third party shall be considered a third-party beneficiary under this DPA, nor shall any third party have any rights as a result of this DPA, except as otherwise provided in the applicable appendix.

6.7 Severability. Should any provision of this DPA be determined invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

6.8 Governing Law and Forum:

(a) Subject to the terms in any applicable Appendices, this DPA shall be governed by and construed in accordance with the laws of England and Wales. The courts of England and Wales shall have sole and exclusive jurisdiction to hear any claims pursuant to this DPA.

(b) Where a specific Appendix identifies a different governing law and forum, such designations will only apply to disputes that arise from the applicable Appendix.

6.9 Termination. Other than with respect to any accrued liabilities of either party and Sections 3.5 and 6.1, this DPA shall terminate automatically on the expiry or termination for whatever reason of the MSA.

Appendix A to the MSA

DESCRIPTION OF THE TRANSFER

Data subjects
The personal data transferred concern the following categories of data subjects:

The data subjects are the data targets of the data exporter. The data subjects may be existing or prospective clients and/or vendors of the data exporter, and individuals who are employees, principals, agents, or representatives of, or otherwise affiliated or associated with, individual or institutional clients and/or vendors, or prospective clients and/or vendors, of the data exporter.

Categories of data
The personal data transferred concern the following categories of data:

Name, address, date of birth, company employment, professional experience and affiliations, wealth data, national security number, Tax ID number, passport number, or other government-issued identification number or code, and such other data that may be transferred from the data exporter to the data importer for the purposes of performing the services pursuant to the MSA.

Special categories of data
The personal data transferred concern the following special categories of data:

Where permitted by law, data importer will process legally reportable criminal convictions and other legally reportable criminal offences; and to the extent revealed in publicly available social media and other processing operations, the sexual orientation, racial or ethnic origin, philosophical beliefs, religious beliefs, political opinions, trade union membership, and sex life of the data subject. Data may also include information relating to minors.

Processing operations (Nature and Purpose)
The personal data transferred will be subject to the following basic processing activities:

- The provision of the Services as detailed within the MSA

Nature: The nature of the data processing activities includes processing activities (e.g., the collection, access, viewing, organizing, disclosing and storing of personal data) as is reasonably required to facilitate and/or support the provision of Services as described under the MSA.

Purpose: The purpose of the data processing activities is to provide hosted software services to be supplied to educational institutions and any other services identified in the MSA.

Certain jurisdiction-specific Appendices to this Personal Data Processing Agreement contain additional details about the transfer of the personal data as required by those jurisdictions.

Appendix B to the MSA

Standard Contractual Clauses for the transfer of personal data from the European Economic Area to third countries

Controller to Processor Transfers

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:
(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries
(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation
(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy
In the event of a contradiction between theses Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)
The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter

throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and personal data records concerned), its likely consequences, and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or

biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers
The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(c) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

9.1 GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2 Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

9.3 The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9.4 The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

9.5 The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights
(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability
(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) **Where the data exporter is established in an EU Member State**: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(a) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(b) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(c) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the

relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities
15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim

measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph(c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will

continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law
These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Romania.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Romania.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEXES

ANNEX I
A. LIST OF PARTIES
B. DESCRIPTION OF TRANSFER
C. COMPETENT SUPERVISORY AUTHORITY

ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

ANNEX III
LIST OF SUBPROCESSORS

ANNEX IV
SWITZERLAND

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. **Name**: Customer, as identified in the MSA to which this Appendix B, and its associated Personal Data Processing Agreement, is appended, on behalf of itself and its affiliated companies to the extent located in the European Union and listed in the MSA.

Address
Contact person's name, position and contact details: Refer to MSA.

Activities relevant to the data transferred under these Clauses: Customer, has appointed the data importer to provide certain advisory, due diligence and/or vetting reports for regulatory purposes, and/or other specified purposes. To facilitate the provision of these services, the data exporters may provide to the data importer access to the personal data described in Annex I.B, below.

Signature and date: This Appendix A is signed by, and on the date of, the Customer's signature to the MSA to which this Appendix A, and its associated Personal Data Processing Agreement, is appended.

Role (controller/processor): Controller

Data importer(s):

1. Name: TnG entity referenced in the MSA.

Address: Address provided in the MSA.

Contact person's name, position and contact details:
Mark Jones,
CEO
mark@teachngo.com

Activities relevant to the data transferred under these Clauses: The data importer(s) is a member of the TnG corporate group and provides the services specified in the MSA. The data importer(s) will process personal data received from the data exporter(s) in order to provide the specific services as described in the MSA.

Signature and date: This Appendix A is signed by, and on the date of, TnG's signature to the MSA to which this Appendix A, and its associated Personal Data Processing Agreement, is appended.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
See Appendix A to the Personal Data Processing Agreement

Categories of personal data transferred
See Appendix A to the Personal Data Processing Agreement

Sensitive data transferred (special categories of personal data)
See Appendix A to the Personal Data Processing Agreement

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal data is transferred on a continuous basis from data exporter to data importer for as long as data importer provides services to the data exporter pursuant to the MSA.

Nature of the processing
See Appendix A to the Personal Data Processing Agreement

Purpose(s) of the data transfer and further processing
See Appendix A to the Personal Data Processing Agreement

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 will be retained for the duration of data importer(s)' performance of services pursuant to the MSA and for as long thereafter as permitted by the MSA unless data importer(s) is/are required by law to delete the personal data sooner.

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

I, applicable,Data importer intends to use the following sub-processor(s) to assist in the performance of its services:

Name of sub-processor: To be provided separately, if applicable.
• Subject Matter:
• Nature of the processing:
• Duration of the processing:

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The applicable Supervisory Authority(ies) is the Supervisory Authority in the country or region where the data exporter(s) is located as of November 2023:

Austria
Österreichische Datenschutzbehörde
Barichgasse 40-421030 Wien
Tel.+43 1 52 152-0
Email: **dsb@dsb.gv.at**
Website: http://www.dsb.gv.at

Belgium

Autorité de la protection des données – Gegevensbeschermingsautoriteit (APD-GBA)
Rue de la Presse 35 – Drukpersstraat 351000 Bruxelles – Brussel

Tel.+32 2 274 48 00
Fax+32 2 274 48 35
Email: contact@apd-gba.be
Website:https://www.autoriteprotectiondonnees.be
https://www.gegevensbeschermingsautoriteit.be

The competence for complaints is split among different data protection supervisory authorities in Belgium. Competent authorities can be identified according to the list provided here:

https://www.autoriteprotectiondonnees.be/citoyen/l-autorite/autres-autorites

https://www.gegevensbeschermingsautoriteit.be/burger/de-autoriteit/andere-autoriteiten

Bulgaria
Commission for Personal Data Protection
2, Prof. Tsvetan Lazarov blvd.1592 Sofia
Tel.+359 2 915 3580+359 2 915 3548
Fax+359 2 915 3525
Email: **kzld@cpdp.bg**
Website: https://www.cpdp.bg

Croatia
Croatian Personal Data Protection Agency
Selska Cesta 13610000 Zagreb
Tel.+385 1 4609 000
Fax+385 1 4609 099
Email: **azop@azop.hr**
Website: http://www.azop.hr

Cyprus
Commissioner for Personal Data Protection
1 Iasonos Street, P.O. Box 233781082 Nicosia
Tel.+357 22 818 456
Fax+357 22 304 565
Email: **commissioner@dataprotection.gov.cy**
Website: http://www.dataprotection.gov.cy

Czech Republic
Office for Personal Data Protection
Pplk. Sochora 27170 00 Prague 7
Tel.+420 234 665 111
Fax+420 234 665 444
Email: **posta@uoou.cz**
Website: http://www.uoou.cz

Denmark
Datatilsynet
Carl Jacobsens Vej 352500 Valby
Tel.+45 33 1932 00
Email: **dt@datatilsynet.dk**
Website: http://www.datatilsynet.dk

Estonia
Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
Tatari 3910134 Tallinn
Tel.+372 6828 712
Email: **info@aki.ee**
Website: http://www.aki.ee

Finland
Office of the Data Protection Ombudsman
P.O. Box 800FI-00531 Helsinki
Tel.+358 29 56 66700
Fax+358 29 56 66735
Email: **tietosuoja@om.fi**
Website: http://www.tietosuoja.fi/en

France
Commission Nationale de l'Informatique et des Libertés – CNIL
3 Place de Fontenoy
TSA 80715 – 75334 Paris, Cedex 07
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Contact: https://www.cnil.fr/en/contact-cnil
Website: http://www.cnil.fr/

Germany
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Graurheindorfer Straße 15353117 Bonn
Tel.+49 228 997799 0
Fax+49 228 997799 5550
Email: **poststelle@bfdi.bund.de**
Website: **http://www.bfdi.bund.de**

The competence for complaints is split among different data protection supervisory authorities in Germany. Competent authorities can be identified according to the list provided under www.bfdi.bund.de/anschriften.

Greece
Hellenic Data Protection Authority
Kifisias Av. 1-311523 Ampelokipi Athens
Tel.+30 210 6475 600
Fax+30 210 6475 628
Email: **contact@dpa.gr**
Website: http://www.dpa.gr

Hungary
Hungarian National Authority for Data Protection and Freedom of Information
Falk Miksa utca 9-11H-1055 Budapest
Tel.+36 1 3911 400
Email: **privacy@naih.hu**
Website: http://www.naih.hu

Iceland
Persónuvernd
Rauðarárstígur 10105 Reykjavík

Tel.+354 510 9600
Email: **postur@dpa.is**
Website: https://www.personuvernd.ishttps://www.dpa.is

Ireland
Data Protection Commission
21 Fitzwilliam SquareD02 RD28 Dublin 2
Tel.+353 76 110 4800
Email: **info@dataprotection.ie**
Website: http://www.dataprotection.ie

Italy
Garante per la protezione dei dati personali
Piazza Venezia, 1100187 Roma
Tel.+39 06 69677 1
Fax+39 06 69677 785
Email: **segreteria.stanzione@gpdp.it**
Website: http://www.garanteprivacy.it

Latvia
Data State Inspectorate
Elijas Street 17LV-1050 Riga
Tel.+371 6722 3131
Fax+371 6722 3556
Email: **info@dvi.gov.lv**
Website: http://www.dvi.gov.lv

Liechtenstein
Data Protection Authority, Principality of Liechtenstein
Städtle 389490 Vaduz
Tel.+423 236 6090
Email: **info.dss@llv.li**
Website: https://www.datenschutzstelle.li

Lithuania
State Data Protection Inspectorate
L. Sapiegos str. 17LT-10312 Vilnius
Tel.+370 5 271 2804+370 5 279 1445
Fax+370 5 261 9494
Email: **ada@ada.lt**
Website: https://vdai.lrv.lt

Luxembourg
Commission Nationale pour la Protection des Données
15, Boulevard du JazzL-4370 Belvaux
Tel.+352 2610 60 1
Fax+352 2610 60 6099
Email: **info@cnpd.lu**
Website: http://www.cnpd.lu

Malta
Office of the Information and Data Protection Commissioner
Second Floor, Airways HouseHigh StreetSLM 1549 Sliema
Tel.+356 2328 7100
Fax+356 2328 7198

Email: **idpc.info@idpc.org.mt**
Website: http://www.idpc.org.mt

Netherlands
Autoriteit Persoonsgegevens
Bezuidenhoutseweg 30P.O. Box 933742509 AJ Den Haag/The Hague
Tel.+31 70 888 8500
Fax+31 70 888 8501
Website: https://autoriteitpersoonsgegevens.nl

Norway
Datatilsynet
Tollbugata 30152 Oslo
Tel.+47 22 39 69 00
Email: **postkasse@datatilsynet.no**
Website: https://www.datatilsynet.no

Poland
Urząd Ochrony Danych Osobowych (Personal Data Protection Office)
ul. Stawki 200-193 Warsaw
Tel.+48 22 531 03 00
Email: **kancelaria@uodo.gov.pl;**
dwme@uodo.gov.pl
Website: https://uodo.gov.pl

Portugal
Comissão Nacional de Proteção de Dados – CNPD
Av. D. Carlos I, 134, 1º1200-651 Lisboa
Tel.+351 21 392 84 00
Fax+351 21 397 68 32
Email: **geral@cnpd.pt**
Website: http://www.cnpd.pt

Romania
The National Supervisory Authority for Personal Data Processing
B-dul Magheru 28-30Sector 1 BUCUREŞTI
Tel.+40 31 805 9211
Fax+40 31 805 9602
Email: **anspdcp@dataprotection.ro**
Website: http://www.dataprotection.ro

Slovakia
Office for Personal Data Protection of the Slovak Republic
Hraničná 12820 07 Bratislava 27
Tel.+ 421 2 32 31 32 14
Fax+ 421 2 32 31 32 34
Email: **statny.dozor@pdp.gov.sk**
Website: http://www.dataprotection.gov.sk

Slovenia
Information Commissioner of the Republic of Slovenia
Dunajska 221000 Ljubljana
Tel.+386 1 230 9730
Fax+386 1 230 9778
Email: **gp.ip@ip-rs.si**

Website: https://www.ip-rs.si

Spain
Agencia Española de Protección de Datos (AEPD)
C/Jorge Juan, 628001 Madrid
Tel.+34 91 266 3517
Fax+34 91 455 5699
Email: **internacional@aepd.es**
Website: https://www.aepd.es

Sweden
Integritetsskyddsmyndigheten
Drottninggatan 295th FloorBox 8114104 20 Stockholm
Tel.+46 8 657 6100
Fax+46 8 652 8652
Email: **imy@imy.se**
Website: http://www.imy.se

Switzerland
Office of the Federal Data Protection and Information Commissioner FDPIC
Feldeggweg 1
CH – 3003 Berne
Tel.: +41 (0)58 462 43 95 (mon.-fri., 10-12 am)
Fax: +41 (0)58 465 99 96
Email: info@edoeb.admin.ch
Website: https://www.edoeb.admin.ch/edoeb/en/home.html

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) 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.

I. ORGANIZATIONAL MEASURES

A. Information Security Governance
Data importer has established a personnel structure for information security governance, including but not limited to, a designated employee with overall responsibility for information security government (e.g., a chief information security officer) and other personnel with assigned roles and responsibilities for information security. Roles and responsibilities have been formally defined for all members of the information security team and have been documented.

B. Administrative Access Controls

1. Access Authorization And Workforce Clearance: An employee or contractor will be authorized to access personal data (“Authorized Users”) only if the individual is deemed trustworthy based upon prior service to the data importer or the successful completion of a background check where permitted by applicable law.

Data importer permits Authorized Users to access personal data only on a need-to-know basis and only as necessary to perform assigned job responsibilities.

2. Confidentiality Agreement: Before establishing access for an Authorized User, data importer requires that the Authorized User execute a confidentiality agreement that applies to the personal data or otherwise acknowledges an obligation of confidentiality.
3. Access Establishment: Data importer separates functions between those authorized to assign access rights and those authorized to establish access to data importer's information systems.
4. Review Of Access Rights: On at least a quarterly basis and when an Authorized User changes positions, data importer reviews and, if necessary, revises or terminated the Authorized User's rights of access to workstations, programs and processes to limit the Authorized User's access to personal data to the minimum necessary to perform assigned job functions. Data importer will delete any personal data stored on the Authorized User's computer that no longer is needed by the Authorized User in his or her new position.
5. Denial Of Access To Terminated Authorized Users: Upon termination of any Authorized User's relationship with data importer, data importer promptly does the following: (a) terminate the Authorized User's rights to access personal data and obtain the return of any devices (such as tokens or key cards) used to obtain access to personal data; (b) obtain the return of all keys, key cards, and other devices that permit access to physical locations containing personal data in paper form; (c) ensure that the terminated Authorized User does not have unescorted access to areas containing personal data in paper form; (d) ensure that all personal data is removed from any computer equipment used by the terminated Authorized User before re-issuing that equipment to another Authorized User.

C. Training

Data importer provides (a) initial training to relevant personnel on how to implement and comply with its information security program, including identifying and reporting a personal data breach, and (b) periodic refresher training and security awareness reminders. Data importer permits newly hired Authorized Users to access personal data only after completion of the initial data security training.

D. Security Incident Response

Data importer has created a security incident response team (SIRT) with assigned roles and responsibilities. Data importer has implemented procedures for identifying security incidents, including personal data breaches, and a plan for responding to security incidents. Data importer periodically tests the security incident response plan. Data importer has established a mechanism for employees to report security incidents, including suspected and actual personal data breaches. Data importer requires all employees to immediately report the loss, theft, or otherwise of any equipment on which personal data is stored.

II. TECHNICAL MEASURES

6. Evaluation And Monitoring

1. Risk Assessment: Data importer has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of personal data. Data importer has implemented policies and procedures to reduce risks and vulnerabilities to personal data to a reasonable

and appropriate level. These policies and procedures are designed to protect the confidentiality, integrity and availability of personal data and to prevent accidental or unauthorized use, disclosure, alteration, loss or destruction.

2. Evaluation Of Security Policies And Procedures: Data importer periodically reviews and, if necessary, updates the policies and procedures described above, as necessary in response to environmental or operational changes affecting the security of personal data.

E. System Activity Review

1. Establishment Of Monitoring Procedures: Data importer has (a) enabled logging on computer systems that store personal data; (b) implemented a process for the review of exception reports and/or logs, and (c) developed and documented procedures for the retention of monitoring data.
2. Monitoring Of System Activity: Data importer periodically reviews information system activity records — including audit logs, access reports, privileged operations, error logs on servers, and security incident tracking reports, and changes to systems security — to ensure that implemented security controls are effective and that personal data has not been potentially compromised. Monitoring includes (a) reviewing changes affecting systems handling authentication, authorization, and auditing; (b) reviewing privileged access to production systems processing personal data; and (c) engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.
3. Compliance Review And Third-Party Audits: Data importer periodically reviews compliance with security policies and procedures. Data importer engages a third party, at least annually, to perform an independent audit which includes an assessment of data importer's information security program. Data importer will make the third-party audit report available to data exporter upon request.

F. Protections Against Malicious Actors

1. Network Security: Data importer maintains an up-to-date firewall and intrusion detection software. Data importer engages in security patch management to ensure that security patches are installed as soon as is reasonably practicable.
2. Anti-Malware Protection: Data importer ensures that protections against malicious software (e.g., anti-virus protection, spyware detection software, etc.) are installed before computers and other devices are connected to any of data importer's networked systems. The software is kept current.

G. Technical Access Controls

1. Unique User ID/Secure Passwords: All Authorized Users will be assigned a unique user ID and will be required to create a strong/complex password, or to use a biometric identifier, to access data importer's network. Systems requiring entry of a password suppress, mask or otherwise obscure the password so that it cannot be viewed by an unauthorized person. All passwords are encrypted while in storage. Authorized Users are required to change passwords on a regular basis. Authorized Users are prohibited form sharing passwords with any other person.
2. Access Restrictions: Data importer has implemented technical controls so that each Authorized User will be able to gain access only to those categories of personal data to which access is necessary to perform assigned job responsibilities.

3. Encryption: Data importer encrypts personal data in transit, using Transport Layer Security (TLS) encryption. Data importer encrypts personal data at rest using 256-bit AES encryption or stronger. Mobile devices and portable electronic storage media used to store personal data must be encrypted.
4. Remote Access: Data importer permits remote access to its networks only via a Virtual Private Network ("VPN") or a similar secure means
5. Secure Disposal: Data importer has established procedures for the secure and permanent destruction of personal data stored in paper and electronic form.

H. Contingency Planning

1. Back-Ups: Data importer backs up personal data on a regular schedule (e.g., at least every 24 hours). Back-ups are encrypted and stored in a location physically apart from the primary storage. Back-ups permit prompt restoration of personal data in the event of a disaster.
2. Business Continuity/Disaster Recovery: Data importer has developed and maintains a business continuity/disaster recovery plan to ensure that data importer can promptly resume service and restore data exporter's access to personal data in the event of a physical or technical incident occurrence (for example, fire, ransomware attack, vandalism, system failure, pandemic flu, and natural disaster).

I. Change and Configuration Management

Data importer maintains policies and procedures for managing changes to production systems, applications, and databases processing personal data and for documenting the changes.

III. PHYSICAL SAFEGUARDS

1. Data importer's facilities where personal data are physically secured against unauthorized access by, for example, keys, access cards, receptionists, and/or security guards. Data importer requires that all employees where a security badge at all time while on data importer's premises. Guests and service providers must register at the reception area and are prohibited from unescorted access to data importer's facility.
2. All servers and network equipment containing personal data are maintained in a location subject to controlled physical access. Only authorized employees may have unescorted access to secure areas where servers and network equipment are located. Video surveillance cameras monitor secured areas where servers and other network equipment are located.
3. Only authorized employees may have unescorted access to areas with computers and other electronic resources that permit access to personal data. Access is restricted by a proximity card or key, receptionist, or some similar method. Physical access rights must be promptly terminated when an employee no longer needs physical access to areas containing electronic resources that permit access to personal data
4. Data exporter requires authorized employees to ensure that all electronic resources permitting access to personal data, including peripherals (computers, monitors, laptop computers, printers, digital cameras, projectors, etc.) that are assigned to, or regularly used by, them are maintained and used in a manner consistent with their function and such that the possibility of damage and/or loss is minimized.

5. Except for equipment designed to be portable, such as laptops, computer equipment used to access personal data should not be removed from data importer's premises without prior authorization.

IV. PERSONAL DATA MANAGEMENT

A. Data Minimization

Data importer has subjected its systems and applications used to process personal data to a review for compliance with privacy-by-design and privacy-default principles and has applied the results of that review to the design of its systems and applications that process personal data. Data importer's systems and applications have been designed to collect, use, disclose, and otherwise process the minimum personal data necessary to provide the services that are the subject of the Parties' underlying agreement. Data importer's systems and applications have been programmed to automatically delete personal data in accordance with data exporter's data retention schedules or data retention instructions unless data importer is required by law to retain personal data for a longer period of time.

B. Accountability

Data importer maintains a record of processing activities ("ROPA") that complies with GDPR, art. 30, with respect to its processing of personal data received form, or created or received on behalf of, data exporter. Data importer makes each relevant ROPA available to data exporter upon request.

C. Data Subject Rights

1. Correction/Update Of Personal Data: Data importer provides self-help options through its website to allow data subjects to correct and update their personal data and/or provides multiple methods (e.g., chat bot, webform, e-mail address) by which data subjects may submit requests for the correction and updating of their personal data.
2. Erasure: Data importer has established internal procedures and technical mechanisms to ensure that personal data can be permanently deleted from production systems and back-ups in response to a request from a data subject, if and to the extent required by GDPR, art. 17.
3. Data Portability: Data importer has implemented procedures and systems that allow data importer to identify Personal Data provided by the data subject and to transfer that personal data, in a usable form, to a third party at the data subject's direction or to the data subject directly or by way of a storage medium.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:
To be specified within the MSA or otherwise communicated between the Parties.

ANNEX IV – SWITZERLAND

Standard Contractual Clauses For The Transfer Of Personal Data From Switzerland To Third Countries
Controller to Processor Transfers

In its communication of August 27, 2021, the Swiss Federal Data Protection and Information Commissioner ("FDPIC") recognised the new SCCs issued by the European Commission in accordance with Regulation (EU) 2016/679 as a legal basis for personal data transfers to a country without an adequate level of data protection, provided that the

necessary adaptations and amendments are made for use under Swiss data protection law. Subsequently on August 31, 2022, the FDPIC announced that the new Federal Act on Data Protection of September 25, 2020 ("nFADP") will enter into force on September 1, 2023. For the purpose of processing of personal data subject to the nFADP, references to the GDPR shall be deemed to be references to the nFADP.

The Standard Contractual Clauses for the Transfer of Personal Data from Switzerland to Third Countries incorporate by reference the Standard Contractual Clauses in this Appendix B and its Annexes I through III for personal data processed by TnG on behalf of Customers located in Switzerland, except that, when transferring Swiss personal data to a third country:

(a) all references to 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 ("GDPR") must be understood and interpreted as references to the nFADP in the context of data transfers abroad that are subject to the nFADP;

(b) any reference to a supervisory authority shall refer to the Swiss Federal Data Protection and Information Commissioner ("FDPIC");

(c) in the event of a data breach, prompt notification to the FDPIC shall be made;

(d) references to a "member state" or to the "EU" in the SCCs shall be deemed to include Switzerland;

(e) appointment of sub processors require the controller's approval; and

(f) with regards to Clauses 17 and 18, these clauses shall be governed by the law of Switzerland and the Customer and TnG agree to the jurisdictions of the courts of Switzerland with regard to any disputes that arise from these Clauses.

Appendix C to the MSA

Terms for Processing Personal Data on behalf of Customers in the United Kingdom when the TnG entity that will be providing services is located outside of the EEA, UK, or Switzerland. Addendum to the EU Standard Contractual Clauses in Appendix B.

International Data Transfer Addendum
to the
EU Commission Standard Contractual Clauses
Part 1: Tables

Table 1: Parties

Start date	The date provided in the MSA to which this Appendix C and associate Personal Data Processing Agreement are appended.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**

Parties' details	Customer as defined the MSA to which this Appendix C and associated Personal Data Processing Agreement are appended, on behalf of itself and its affiliated companies to the extent located in the UK Main address: Customer's Address Official registration number (if any) (company number or similar identifier): Customer's registration number	TnG Entity Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name: Customer Contact Job Title: Contact details including email: Customer email address	Full Name: Mark Jones CEO mark@teachngo.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs, Appendix B, which this Addendum is appended to, detailed below, including the Appendix Information: Date:

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: TnG Entities
Annex 1B: Description of Transfer: Transfer of Personal Data between TnG Entities for legitimate purposes to facilitate certain necessary transactions.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Parties shall comply with responsibilities under the Data Transfer Agreement including EU SCCs
Annex III: List of Sub processors (Modules 2 and 3 only): As provided in the Data Processing Agreement

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: X Importer X Exporter

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 12, 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. 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.

Appendix D to the MSA

Other than the terms defined in this Section I, capitalized terms have the definition provided in the Personal Data Processing Agreement to which this Appendix D is appended.

"Discover," with respect to a Personal Data Breach, means knowledge by any member of TnG's workforce — other than the person responsible for the Personal Data Breach —

that the Personal Data Breach has occurred.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed when that Personal Data is in the possession of TnG or its agents or subcontractors.

“Required By Law” means that a statute, regulation, court order, or legal process, enforceable in a court of law, mandates the conduct.

“Sensitive Personal Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, sex life, or sexual orientation, genetic data and biometric data when Processed for the purpose of uniquely identifying a natural person, and also includes information about criminal history.

“European Data Processing Agreement” means these Terms for Processing Personal Data within the European Economic Area (“EEA”), Switzerland, and the UK (Appendix D) and its attachments.

TnG’s Processing Of Personal Data

Nature and Purpose Of Processing of Personal Data. TnG agrees to Process Personal Data in accordance with Attachment 1, which describes the nature and purpose of the Processing, the type of Personal Data, and the categories of Data Subjects.

Violation Of The Law. Customer will not direct TnG to Process Personal Data in violation of TnG’s or Customer’s obligations under applicable data protection law. TnG will promptly notify Customer if TnG discovers that TnG’s compliance with a term or condition of this European Data Processing Agreement has violated, violates, or would violate TnG’s or Customer’s obligations under applicable law.

Disclosures Of Personal Data As Required By Law. Before TnG discloses Personal Data as Required By Law, TnG will, unless prohibited by the legal requirement from doing so, notify Customer and permit Customer adequate time to exercise its legal options to prevent or limit disclosure of Personal Data before TnG discloses any Personal Data.

TnG’s Safeguards For Personal Data

Confidentiality Of Personal Data. TnG will maintain the confidentiality of all Personal Data. TnG will permit its employees to Process Personal Data only after undergoing appropriate training and acknowledging their confidentiality obligation with respect to that Personal Data.

Physical, Technical And Organizational Safeguards. TnG shall maintain an information privacy and security program that includes reasonable and appropriate measures — including technical, physical, and organizational safeguards taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons — to protect against reasonably foreseeable risks to the security, confidentiality, integrity and resilience of Personal Data, which risks could result in the unauthorized disclosure, use, alteration, destruction or other compromise of the Personal Data, including a Personal Data Breach.

Reporting Personal Data Breaches. TnG will report to Customer any Personal Data Breach discovered by TnG, as soon as reasonably practicable.

Cooperation in Investigation And Mitigation. TnG agrees to cooperate with Customer in its investigation of any Personal Data Breach. TnG will take reasonable and appropriate steps to mitigate the known, adverse effects of a Personal Data Breach.

TnG's Assistance With Audits And Requests From Data Subjects

Availability Of Records Of Processing. TnG will, upon reasonable, written request from Customer, promptly make available to Customer information necessary to demonstrate Customer's compliance with its obligations established by applicable law.

Information Technology Audits. Upon fifteen (15) business days' prior written notice, TnG will permit Customer, directly or through a contractor, to conduct site audits of the information technology used to Process Personal Data and of TnG's information security controls for Personal Data. Before commencement of the audit, Customer and, where applicable, Customer's selected contractor must enter into an appropriate confidentiality agreement with TnG.

Requests For Impact Assessment Information. TnG will provide the information reasonably requested by Customer to assist Customer in conducting a data protection impact assessment pursuant to applicable law.

Requests From Data Subjects. TnG agrees to assist Customer in responding to a request from a Data Subject to exercise their individual rights which may include the right to access, rectify, or erase his/her Personal Data, to restrict or block the Processing of his/her Personal Data or for data portability with respect to his/her Personal Data ("Data Subject Request"). In the event a Data Subject submits a Data Subject Request directly to TnG, TnG will notify Customer of the Data Subject Request and will await instructions from Customer regarding its response to the Data Subject Request. Upon receipt of Customer's written instructions, TnG will take such action reasonably requested by Customer to assist Customer in responding to the Data Subject Request.

TnG's Sub-Processors

Consent To Processing By Sub-Processors. Customer consents to TnG's use of the sub-processors identified in Attachment 2 appended hereto or as otherwise communicated from time to time. Customer consents to TnG's engaging additional or different sub-processors to Process Personal Data provided that TnG notifies Customer of such proposed sub-processor and gives Customer a reasonable opportunity (which shall not exceed ten (10) business days) to object. TnG shall remain responsible for, and remain liable to, Customer for, the acts and omissions of its sub-processor with regard to their Processing of Personal Data as if they were TnG's own acts and omissions. In the event Customer objects to TnG's disclosure of Personal Data to a sub-processor, TnG may terminate this European Data Processing Agreement and the MSA without liability.

Sub-processors' Physical, Technical And Administrative Safeguards. TnG will obtain reasonable assurances, in writing, from any sub-processor to whom TnG discloses Personal Data that the sub-processor will comply with substantially the same restrictions and conditions on Processing Personal Data that this European Data Processing Agreement imposes on TnG.

Miscellaneous Terms

Modification. The Parties agree to amend this European Data Processing Agreement and/or the MSA from time to time as may be necessary to permit Customer to remain in compliance with applicable law.

ATTACHMENT 1: DESCRIPTION OF THE TRANSFER
ATTACHMENT 2: SUB-PROCESSORS

ATTACHMENT 1:
DESCRIPTION OF THE TRANSFER

Nature Of Processing By TnG:

See Appendix A to the Personal Data Processing Agreement

Purposes Of Processing By TnG:

See Appendix A to the Personal Data Processing Agreement

Categories of Data Subjects Whose Personal Data Is Processed By TnG:

See Appendix A to the Personal Data Processing Agreement

Categories Of Personal Data Processed By TnG:

See Appendix A to the Personal Data Processing Agreement

Special Categories Of Personal Data Processed By TnG (Sensitive Personal Data):

See Appendix A to the Personal Data Processing Agreement

ATTACHMENT 2:
SUB-PROCESSORS

Customer agrees to TnG's use of the following sub-processors to Process Personal Data:

[To Be Provided Separately]

Appendix E to the MSA
California Privacy Rights Act Agreement

AGREEMENT

Commencing on January 1, 2023, the following provisions apply to TnG's Collection, retention, use, disclosure, and other handling, (collectively, "processing") of the Personal Data of Consumers:

a. Definitions: Unless otherwise indicated in this California Privacy Rights Act Agreement ("CPRA Agreement"), the capitalized terms used in this CPRA Agreement shall have the

meaning assigned to them in the California Privacy Rights Act ("CPRA").
6.

i. "**Consumer**" means a California resident (a) who is a natural person and (b) whose Personal Data is processed by TnG on behalf of Customer for the purposes of the MSA.

ii. **"Categories of Personal Data"** or "Category of Personal Data" shall mean the categories or category, respectively, of Personal Information listed in Cal. Civ. Code §1798.140(v)(1).

iii. **"CPRA Regulations"** shall mean final regulations implementing the CPRA after those regulations go into effect.

iv. **"Permitted Subcontractor"** means TnG's subcontractor that agrees, by written contract, to the same restrictions and prohibitions on the processing of Personal Data that this CPRA Agreement imposes on TnG.

v. **"Personal Data"** shall have the definition of "personal information" set forth in the CPRA but shall be limited to the personal information of Consumers.

vi. **"Sensitive Personal Data"** shall have the definition of "sensitive personal information" set forth in the CPRA but shall be limited to the personal information of Consumers.

b. Compliance With Applicable Law: TnG shall process Personal Data only (i) in accordance with the CPRA and all other applicable laws and regulations, and (ii) in a manner that provides the same level of protection for Personal Data as the CPRA requires Customer to provide. Customer may take reasonable and appropriate steps to help ensure that TnG uses Personal Data consistent with the CPRA. TnG will notify Customer if TnG determines that it can no longer meet its obligations under the CPRA.

c. Permissible Processing Of Personal Data: TnG shall process Personal Data only (a) on Customer's behalf, (b) for Customer's Business Purposes, and (c) to help Customer respond, pursuant to subparagraph (g), below, to a request by a Consumer to exercise rights under the CPRA; and (d) for any other purpose explicitly permitted under the CPRA or its implementing regulations.

d. Restrictions On Processing Personal Data: TnG is prohibited from (i) processing Personal Data for any purpose other than to perform the Services, including any other commercial purpose; (ii) otherwise processing Personal Data outside the direct business relationship between Customer and TnG; (iii) Selling or Sharing Personal Data; (iv) combining Personal Data with personal information that it receives from, or on behalf of, another person or persons, or Collects from its own interaction with a California Consumer (except as permitted by the CPRA's Regulations); or (v) processing the Personal Data for any other purpose except as permitted by this CPRA Agreement.

e. Restrictions On Disclosure Of Personal Data To Subcontractors: TnG engages subcontractors to process Personal Data on TnG's behalf. TnG shall not disclose any Personal Data to any subcontractor, or permit any subcontractor to create, process, or receive Personal Data on TnG's behalf, unless the subcontractor is a Permitted Subcontractor.

f. Requests By An Individual Directed To TnG: TnG shall refer to Customer, within three (3) business days of receipt, any request received by TnG directly from a Consumer for:

(i) deletion, correction, or specific pieces, of Personal Data related to the Consumer retained by the TnG or the TnG's subcontractors; (ii) disclosure regarding the Personal Data about the Consumer, if any, that TnG Collects, discloses for a Business Purpose, Sells, or Shares; (iii) opt-out of the Sale or Sharing, if any, of the Consumer's Personal Data; or (iv) restriction of the use or disclosure of Sensitive Personal Data. TnG shall await instructions from Customer before acting upon any request received directly from a Consumer.

g. Cooperation With Customer's Response To Requests From Consumers: Within twenty-five (25) days of receiving a request from Customer for assistance in responding to a request by a Consumer to exercise one or more of the rights provided by the CPRA, TnG shall do the following, as applicable:

i. (A) delete the Consumer's Personal Data from the TnG's records and (B) notify any of its subcontractors and any Third Parties with which TnG shared the Consumer's Personal Data to delete the Consumer's Personal Data unless this proves impossible or involves disproportionate effort;

ii. correct the Consumer's Personal Data as directed by Customer, unless: (A) the TnG believes that the Personal Data is already correct, in which case TnG will provide an explanation in writing to Customer of why the Personal Data is already correct and, if Customer responds by directing TnG to revise the Personal Data, TnG revise the Personal Data as directed by Customer; or (B) TnG warrants, and responds in writing, that the Personal Data is in an archived record that TnG does not use as a source of accurate Personal Data and does not share with Third Parties;

iii. identify:

A. the Categories of Personal Data, and specific pieces of Personal Data, Collected about the Consumer;

B. the categories of sources from whom the Consumer's Personal Data is Collected, if the sources are other than Customer;

C. the Business Purpose or Commercial purpose for Collecting, Selling, or Sharing the Consumer's Personal Data; and

D. the categories of entities or individuals, other than Permitted Subcontractors, to which the TnG disclosed the Consumer's Personal Data;

iv. provide Customer with a copy of the specific pieces of Personal Data Collected about the Consumer if Customer does not already have a copy of the specific pieces of Personal Data requested;

v. identify (A) the Consumer's Categories of Personal Data Sold or Shared, and (B) for each Category of Personal Data Sold or Shared, the entities or individuals to which that Category of Personal Data was Sold or Shared;

vi. identify (A) each entity or individual to whom the TnG has disclosed the Consumer's Personal Data for a Business Purpose, (B) the Categories of Personal Data disclosed, and (C) the Business Purpose(s) for the disclosure; and/or

vii. follow Customer's instructions regarding any limitations on the use or disclosure of the Consumer's Sensitive Personal Data.

7. Customer will pay TnG’s charges for providing assistance in responding to a request by a Consumer to exercise one or more of the rights provided by the CPRA, at TnG’s standard consultancy rates.