Data Processing Addendum (for personal data governed by the GDPR)

RECITALS

A. This Addendum applies to, and forms part of, any agreement that expressly incorporates this Addendum into it by reference (**Agreement**).

B. This Addendum only applies to personal data processed by the Company as processor (or by its subprocessors) for the Customer in connection with the Agreement about the Customer's employees, officers, agents, students and/or End Users (**Data Subjects**) that is governed by the *General Data Protection Regulations (EU) 2016/679* (the **GDPR**).

C. It does not apply to any other personal data.

THE PARTIES AGREE AS FOLLOWS:

1 Definitions and Interpretation

1.1. In this Addendum:

(a) any words starting with a capital letter shall have the meanings given to them in the Agreement unless otherwise defined in this Addendum;

(b) **Data Breach Response Plan** means any Security and Data Breach Response Plan implemented by the Company from time to time;

(c) **process** (and other forms of that word) has the meaning given to 'processing' in the GDPR;

(d) **subprocessor** means any natural or legal person, public authority, agency or other body appointed by the Company to process personal data of Data Subjects on behalf of the Company that the Company has been appointed to process as a processor by the Customer; and

(e) the words '**controller**', '**processor**', '**personal data**', '**processing**', '**personal data breach**', and '**supervisory authority**' have the meanings given to them in the GDPR.

1.2. Interpretation

(a) the rules of interpretation set out in the Agreement apply to this Addendum, except where inconsistent with the GDPR, in which case the interpretation provisions of the GDPR will prevail; and

(b) the recitals to this Addendum form part of its operative binding terms.

2 Compliance with the GDPR

2.1. The Customer (as controller) hereby appoints the Company as a processor to process the personal data of Data Subjects described in the Agreement for the purposes described in the Agreement.

2.2. Each party hereby agrees that it will comply with its obligations under the GDPR, including by collecting, disclosing and otherwise processing personal data of Data Subjects in accordance with the GDPR and by maintaining all records and information required by the GDPR.

2.3. The Customer must not provide any instructions to the Company with respect to personal data of Data Subjects that contravenes the GDPR.

2.4. The Company shall promptly notify the Customer if it forms the view that, in its reasonable opinion, an instruction provided by the Customer infringes the GDPR (unless that notification would breach Applicable Law).

2.5. The Customer hereby instructs the Company to process personal data of Data Subjects, as required by the Company to exercise its rights or comply with its obligations under the Agreement.

2.6. The Customer must provide the Company with any information and otherwise cooperate with the Company, to the extent reasonably required by the Company to comply with its obligations under the GDPR.

2.7. Appendix 1 to this Addendum sets out operable provisions of this Addendum that form part of the Agreement for the purposes of Article 28(3) of the GDPR.

3 Data Transfers

3.1. If any personal data of any Data Subject originates from the European Economic Area (**EEA**) or the United Kingdom under the Agreement, the parties shall execute applicable Standard Contractual Clauses (the **Model Clauses**), with the Customer as the "Data Exporter," which such executed Model Clauses shall be incorporated into this Agreement by reference. If any personal data originates from any country (other than an EEA country) with laws imposing data transfer restrictions and the Customer has informed the Company of such data transfer restrictions, the Customer and the Company shall ensure an appropriate transfer mechanism (satisfying the country's data transfer requirement(s)) is in place, as mutually

agreed upon by both parties, before transferring or accessing personal data outside of such country. For the avoidance of doubt: (a) these transfer provisions do not pertain to End Users who have access to the Services and personal data; (b) the Company is not responsible for the actions of End Users; and (c) the Customer is solely responsible for ensuring that any use of the Services and access to personal data by End Users is compliant with Applicable Law.

3.2. The Customer must ensure that End Users do not use the Software or Services in any country with laws that would require personal data to be hosted in that country.

3.3. The Company must ensure that personal data is not accessed or transferred outside the EEA ,or countries covered by a data privacy framework for the flow of personal data outside the EEA, by Company staff unless otherwise authorised by Customer.

4 Confidentiality

4.1. The Company will use its best endeavours to procure that all of its employees who access personal data of any Data Subject whose personal data is processed by the Software:

(a) are subject to contractual confidentiality obligations or professional or statutory obligations of confidentiality; and

(b) do not cause the Company to breach the GDPR.

5 Security

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall, and shall procure that its subprocessors shall, with respect to personal data of any Data Subject processed by the Software, implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2. In assessing the appropriate level of security, the Company shall take into account the risks that are presented by processing, in particular the risk of, or occurrence of, a personal data breach.

5.3. For the purposes of clauses 5.1 and 5.2 of this Addendum, the technical and organisational measures that the Company has implemented, and will continue to implement, for the Term of the Agreement to protect personal data of Data Subjects against unauthorised or unlawful processing and against accidental loss, destruction or damage, are as follows:

(a) ensuring the confidentiality, integrity and availability of its information assets and information systems;

(b) applying a consistent Information Security framework across the Company aligned with the ISO 27001 "Information Security Management System" standard;

(c) ensuring all applicable staff and contractors are aware of their information security responsibilities and that they are appropriately trained to meet those responsibilities;

(d) only using reputable hosting providers to host personal data;

(e) implementing passwords and access control procedures into its computer systems;

(f) performing security testing (including penetration testing of its Software) and maintaining other electronic (e-security) measures for the purposes of securing personal information, such as passwords, anti-virus management and firewalls;

(g) having an information security management framework;

(h) maintaining physical security measures in its buildings and offices such as door and window locks and visitor access management, cabinet locks, surveillance systems and alarms to ensure the security of information systems (electronic or otherwise);

(i) having a Data Breach Response Plan in place;

(j) having data backup, archiving and disaster recovery processes in place; and

(k) Ensuring data is encrypted in transit and at rest with encryption keys managed and stored within the EEA.

5.4. The Customer agrees that the technical and organisational measures set out in clause 5.3 satisfy the Company's obligations under clauses 5.1 and 5.2.

6 Subprocessing

6.1. The Customer hereby authorises the Company to engage any third-party vendor, contractor or service provider as a subprocessor in connection with the provision of the Software and Services (and in connection with the provision of any ancillary services), including any hosting provider selected by the Company. Subprocessors may include partners, affiliates, suppliers and hosting providers. The Company will not appoint (or disclose any personal data to) any subprocessor unless required in order for the Company to exercise its rights or comply with its obligations under the Agreement or to comply with Applicable Law.

6.2. Subject to clause 6.3, the Company is authorised to continue to use those subprocessors already engaged by the Company as at the date of this Addendum (**Approved subprocessors**). ReadyTech subprocessor list is available at https://readytech.io/subprocessors/.

6.3. The Company will provide prior written notice to the Customer of the proposed appointment of any new subprocessor (whether or not to replace any Approved subprocessors) (each, a **New subprocessor**) after the date of the Agreement. If, within 10 calendar days following receipt of that notice by the Customer, the Customer notifies the Company in writing of any objections to the proposed appointment, the parties will endeavour to agree in good faith, without undue delay, the steps to be taken to ensure that such objections are addressed and the Company shall not appoint that proposed New subprocessor until such time as appropriate steps have been taken to address the objections raised by the Customer.

6.4. The Company shall:

(a) have or will enter into written agreements with its subprocessors who are appointed by the Company to process personal data of Data Subjects in connection with the Agreement, as between each subprocessor and the Company governing the obligations regarding processing of personal data; and

(b) as between the Company and the Customer, be liable for any breach by a subprocessor of the subprocessor's data protection obligations under the GDPR in connection with such personal data of Data Subjects.

6.5. The Customer may request from the Company a list of subprocessors engaged by the Company for the purposes of the Agreement. The Company shall make such a list available to the Customer.

7 Data Subject Rights

7.1. Having regard to the nature of the processing, the Company shall, insofar as it is possible, assist the Customer by implementing appropriate technical and organisational measures to respond to requests from Data Subjects who wish to exercise their rights under the GDPR.

7.2. To the extent the Customer is not able to correct, amend, modify, or delete Data Subject personal data using functionality in the Software, the Company shall comply with any commercially reasonable request by the Customer to facilitate such assistance to the extent the Company is legally obligated to do so by the GDPR.

7.3. The Company shall promptly notify the Customer if the Company receives a request from a Data Subject to exercise any of their rights under the GDPR with respect to personal data of the Data Subject processed by the Company in connection with the Agreement.

8 Deletion or return of Personal Data

8.1. Following termination of the Agreement, the Customer shall have thirty (30) days to export the personal data of Data Subjects from the Software and after such time has passed the Company may destroy all personal data of Data Subjects processed by the Company in connection with the Agreement in its possession or control. This requirement shall not apply:

(a) to the extent that the Company is required by Applicable Law to retain some or all of the personal data, provided that the Company shall continue to protect such data in accordance with its obligations set out in this Addendum; or

(b) to the extent that the Company has collected the personal data in its capacity as a controller.

9 Personal data breaches

9.1. The Company shall notify the Customer as soon as possible upon the Company becoming aware of a personal data breach that requires notification to a Data Subject, that there has been a personal data breach together with sufficient information (to the extent known by the Company) to allow the Customer to meet its obligations to notify Data Subjects of the personal data breach. The current assigned Data Processing Officer at ReadyTech is M.

Nickels – Head of Security Operations and can be contacted via (security@readytech.io).

9.2. The Company shall co-operate with the Customer and take such reasonable commercial steps as are reasonably requested by the Customer to assist the Customer with the investigation of each such personal data breach.

9.3. The Customer must notify Data Subjects and any applicable supervisory authority of any applicable data breaches in accordance with the GDPR. If the Customer does not notify Data Subjects or any applicable supervisory authority of an applicable personal data breach (where such notification is required) the Company may discharge its obligations under the GDPR by making any notifications to those Data Subjects or the applicable supervisory authority that it may be required to make.

10 Data Protection Impact Assessments

10.1. The Company, shall, upon the Customer's request, to the extent that the Customer does not otherwise have access to the relevant information through the Software or otherwise, and such information is readily available to the Company, provide reasonable assistance to the Customer to enable the Customer to carry out data protection impact assessments as required by the GDPR taking into account the nature of the processing and the information available to the Company.

11 Indemnity

11.1. The Customer must indemnify the Company from and against any loss or damage incurred by the Company as a result of:

(a) the Customer's breach of the GDPR; or

(b) the Company's compliance with the Customer's instructions with respect to the processing of personal data.

12 Information requested by the Customer

12.1. Upon the Customer's request and in any event only once in any 12 month period of the Term, the Company will, following a request for same by the Customer, make available to the Customer all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR (to the extent that the Customer has not already been provided with or is in possession of such information).

12.2. The Customer acknowledges that any information provided by the Company to the Customer pursuant to clause 12.1 is the Company's Confidential Information, and the Customer shall protect such information in accordance with the confidentiality provisions of the Agreement.

13 Limitation of Liability

13.1. The Customer's remedies arising out of or related to this Addendum (and, to the extent executed by the parties, the Model Clauses) will be subject to those limitations of liability that limit the liability of the Company under the Agreement, and the aggregate liability of the Company to the Customer under the Agreement, this Addendum and the Model Clauses in relation to the processing of personal data of Data Subjects shall not exceed (in the aggregate) the maximum liability of the Company to the Customer under the Agreement.

13.2. The Company is not liable for any claim brought by the Customer or any third party (including, without limitation, any Data Subject, or regulatory or supervisory authority) to the extent arising from the Company's compliance with the Customer's instructions with respect to the processing of personal data.

Appendix 1

Details of processing under Article 28(3) of the GDPR

Article 28(3) Requirement	The Company's data processing details
Subject matter and the duration of processing	The Company will process personal data of Data Subjects in order to comply with its obligations and exercise its rights under the Agreement and in order to comply with Applicable Law. This will occur for the Term of the Agreement.
Nature and purpose of the processing	The Company will process personal data of Data Subjects for the purpose of providing End Users with access and use of the Software and its functionality (including administration, operations, technical and customer support) in accordance with the Agreement and to exercise the Company's rights and for the Company to comply with Applicable Law.
Types of personal data to be processed	Data Subjects: All information, including personal data, that is entered into the Software (either by End Users or otherwise). The types of personal data collected may include names, contact details, employment information and payroll data, as well as any other personal data entered into the Software by, about or on behalf of a Data Subject. Personnel of the Customer: contact and billing details of the Customer's Personnel.
The categories of Data Subjects to whom the personal data relates	The categories of Data Subjects to whom the personal data relates include: (a) all individuals (including End Users and otherwise) about whom data is uploaded or entered into the Software or provided to the Company, on behalf of the Customer; and (b) Personnel of the Customer.
Processing of special categories of personal data	End Users of the Software may upload and/or enter special categories of personal data, where the functionality of the Software is designed to process such data (where expressly permitted by the Agreement).
Obligations and rights of the controller	The Customer must comply with its obligations under the GDPR and all other Applicable Law. Its contractual obligations to the Company are set out in the Agreement.