

Data Processing Agreement

This Data Processing Agreement (“**DPA**”) is subject to the Master License & Services Agreement or its equivalent (the “**Agreement**”) and applicable Ordering Document or its equivalent (the “**Order**”) executed by and between Maverick Training Corporation, d/b/a Maverick Solutions (“**Maverick**”) and (a) the entity identified in the applicable Order as the recipient of the license to the Application and, as applicable, (b) the reseller of the license to the Application (“**Client**”). Capitalized terms used but not defined herein shall have the meanings ascribed to such terms in the Agreement and Order.

If there is any inconsistency between the terms of the Agreement and this DPA, this DPA shall prevail.

1. **Definitions.**

- a. “**Applicable Data Protection Law**” means all applicable data protection laws, rules and regulations protecting the personal data of natural persons that is applicable to the processing of Client Personal Data including, without limitation, the GDPR, CCPA and any national legislation which supplements the GDPR, the CCPA, and the data protection laws of any other country, state or territory which apply to such processing;
- b. “**CCPA**” means the California Consumer Privacy Act of 2018, on the protection of California residents with regard to the Processing of Personal Information, Cal. Civ. Code §§ 1798.100 *et seq.*, as amended, and its implementing regulations;
- c. “**EEA SCCs**” means the standard contractual clauses set out in the European Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as updated, amended, replaced or superseded from time to time by the European Commission;
- d. “**GDPR**” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data;
- e. “**Restricted Transfer**” means a transfer of Personal Data from Client to Maverick, where such transfer would be prohibited by Applicable Data Protection Laws in the absence of the Standard Contractual Clauses;
- f. “**Standard Contractual Clauses**” means either the EEA SCCs or UK IDTA, as applicable to a Restricted Transfer.

- g. **“UK GDPR”** means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.
- h. **“UK IDTA”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under Section 119A(1) Data Protection Act 2018, as updated, amended, replaced or superseded from time to time by the UK Government; and
- i. **“Business,” “Controller,” “Processor,” “Data Subject,” “Personal Data,” “Personal Information,” “Personal Data Breach,” “Processing,” “Service Provider” and “Sub-Processor”** shall have the means given them under Applicable Data Protection Laws. **“Processed,” “Processes” and “Process”** shall be construed in accordance with the definition of **“Processing”**.

2. **Roles of the Parties.** For purposes of Applicable Data Protection Law, Maverick acts as a Data Processor or Service Provider, as applicable, of Client Personal Data on behalf of Client. Client agrees that (i) it shall comply with its obligations as a Controller or a Business, as applicable, under Applicable Data Protection Laws in respect of its Processing of Personal Data and any Processing instructions it issues to Maverick; and (ii) it has provided notice and obtained (or shall obtain) all rights necessary under Applicable Data Protection Laws for Maverick to Process Client Personal Data, including, without limitation, all consents necessary, and provide the Services pursuant to the Agreement and this DPA.
3. **Scope and Details of Client Personal Data Processing.** The subject-matter and duration of the Processing of Client Personal Data, the nature and purpose of the Processing, the types of Client Personal Data and categories of Data Subjects are set out in Appendix 1 to this DPA.
4. **Processing of Client Personal Data.** Maverick will Process Client Personal Data only on documented instructions from Client, including with regard to transfers of Client Personal Data to a third country, unless Maverick is required to Process the Personal Data by an applicable law to which Maverick is subject. In such case, Maverick shall inform Client of that legal requirement before Processing, unless that law prohibits providing such information. Maverick shall immediately inform Client if, in Maverick’s reasonable opinion, an instruction from Client infringes Applicable Data Protection Laws.
5. **Confidentiality.** Maverick agrees that Client Personal Data shall be Confidential Information as that term is defined under the Agreement and ensures that any individual who is authorized to access to Client Personal Data will be required to keep such data confidential, such as through a confidentiality agreement or an acceptable use policy.

- 6. Security.** 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 impact on the individuals to whom Client Personal Data relates, Maverick shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk as identified in Applicable Data Protection Laws, which are outlined in Appendix 2.
- 7. Personal Data Breach.** Maverick will comply with the Personal Data Breach-related obligations directly applicable to it under Applicable Data Protection Laws and, taking into account the nature of Processing and the information available to Maverick, will assist Client in complying with Client's obligations under Applicable Data Protection Laws.
- 8. Sub-processing.** Maverick may subcontract the collection or other Processing of Client Personal Data only in compliance with Applicable Data Protection Laws. Client hereby authorizes Maverick to use Sub-Processors. Maverick may continue to use those Sub-Processors already engaged by Maverick as of the effective date of this DPA (see Appendix 3), subject to Maverick in each case as soon as reasonably practicable meeting the obligations set out in this Section 8. Maverick will notify Client of any planned additions to or replacements of the Sub-Processors and Client may object to such alterations by providing written notice within ten (10) days. If Client objects to the new Sub-Processor, the Parties will work together in good faith to first resolve the reason(s) for the objection and then, if a resolution cannot be reached, find an alternative Sub-Processor. If the Parties are unable to identify an alternative Sub-Processor within thirty (30) business days from the date upon which Client objected, then both Parties will have the right to terminate this DPA and the Agreement, subject to any termination fees outlined therein. Where Maverick engages another processor for carrying out specific processing activities on behalf of Client, Maverick shall make reasonable efforts to impose on that other processor the same data protection obligations as set out in this DPA. Where the Sub-Processor fails to fulfil its data protection obligations, Maverick shall remain fully liable to Client for the performance of that Sub-Processor's obligations.
- 9. Data Subject Requests.** Taking into account the nature of the Processing, Maverick will assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to requests by individuals for exercising their rights under Applicable Data Protection Laws. Client also agrees that, to the extent legally permitted, Client shall be responsible for any costs arising from Maverick's provision of such assistance. For the avoidance of doubt, the assistance that may be provided by Maverick to Client in responding to data subject requests does not constitute any obligation by Maverick to respond to such request; Client is solely responsible for responding to data subject requests.
- 10. Reasonable Assistance.** Maverick will assist Client, at Client's costs, in ensuring Client's compliance its obligations under Applicable Data Protection Laws, as relevant to Maverick's

role in Processing the Personal Data, taking into account the nature of Processing and the information available to Maverick.

11. Deletion of Client Personal Data. Except as otherwise may be agreed upon in the Agreement, upon termination of the Agreement or the provision of the services thereunder relating to the Processing of Client Personal Data, Maverick will delete all Client Personal Data, including all copies of such Client Personal Data, except to the extent that Applicable Data Protection Law requires storage of the Client Personal Data.

12. Audit Rights. Client may, at Client's expense, but no more than once annually, conduct a reasonable audit or inspection of Maverick to ensure compliance with Maverick's obligations under this DPA. Maverick will make available to Client all information that is necessary to demonstrate such compliance. Client shall reimburse Maverick for any time expended for any such audit at Maverick's then-current professional services rates. Before the commencement of any such audit, Client and Maverick shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Client shall be responsible.

13. Cooperation with Supervisory Authorities. Client and Maverick shall cooperate with competent Supervisory Authorities as required by the Applicable Data Protection Laws. If a party is subject to investigative or corrective powers of a Supervisory Authority, this party shall inform the other party without undue delay, insofar as it relates to the data Processing covered by this DPA. The Parties shall provide reasonable assistance to each other to fulfill obligations to cooperate with Supervisory Authorities. Each party is responsible for its own costs arising from the provision of such assistance.

14. Processing of Personal Information Subject to the CCPA. In connection with Maverick's provision of Services to Client under the Agreement if Maverick receives any Client Personal Data that qualifies as Personal Information (as defined in the CCPA) from or on behalf of Client, then Maverick: (a) will only process such Personal Information for the purpose of providing such Services (including as permitted in Appendix 1 hereto); (b) will not retain, use, or disclose such Personal Information for any purpose (i) other than to perform the Services or (ii) outside of the direct business relationship between Maverick and Client; (c) will not sell, share, rent, release, disclose, disseminate, make available, transfer or otherwise communicate such personal information to any third party for monetary or other valuable consideration; and (d) certifies that it understands the restrictions on its processing of such Personal Information as set forth in this sentence, and will comply with them. Maverick may disclose such Personal Information to Maverick's Service Providers in connection with such Service Providers providing services to Maverick, and Maverick may permit such Service Providers to Process such Personal Information as necessary for Maverick to provide the Services to Client.

15. Transfers Outside of EEA+ or UK.

- a. In respect to any Restricted Transfer subject to the GDPR, the Parties hereby enter into Module Two of the EEA SCCs with Client as data exporter and Maverick as data importer. The EEA SCCs are hereby incorporated by reference into this DPA. The Parties make the following selections for the purposes of Module Two:

- i. **Clause 7** – Docking clause shall apply;
- ii. **Clause 9** – Use of sub-processors: Option 2 shall apply and the “time period” shall be 30 days;
- iii. **Clause 11(a)** – Redress: the optional language shall not apply;
- iv. **Clause 13(a)** –

- 1) Where Client is established in an EU Member State, the following shall apply:
“The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall be the supervisory authority of the Member State in which Client is established or (if different) the lead supervisory authority of the Client in respect of a cross-border processing activity”.

OR

- 2) Where Client is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR, the following shall apply: “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, shall act as competent supervisory authority.”

OR

- 3) Where Client is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) without however having to appoint a representative the following shall apply: “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.”

- v. **Clause 17** – Governing law: “Option 1” shall apply and the “Member State” shall be the Republic of Ireland;
- vi. **Clause 18** – Choice of forum and jurisdiction: the Member State shall be the Republic of Ireland;
- vii. **Annex I** – See Appendix 1.
- viii. **Annex I.C.** – Competent Supervisory Authority: Republic of Ireland
- ix. **Annex II** – See Appendix 2.
- x. **Annex III** – N/A.

- b.** In respect to any Restricted Transfer subject to FADP, the Parties hereby enter into Module Two of the EEA SCCs with Client as data exporter and Maverick as data importer. The EEA SCCs are hereby incorporated by reference into this DPA. The Parties make the same elections as outlined in Section 15.a. above, with the following addition modifications:
- i.** References to the GDPR shall be interpreted as references to the Swiss Federal Act on Data Protection of June 19, 1992 (“FADP”) or by any subsequent act, including the relevant amendments and implementing ordinances (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established).
 - ii.** “personal data”, “special categories of data/sensitive data”, “personality profiles”, “profiling” “profiling with high risk”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the meaning assigned to them by the Swiss Federal Act on Data Protection of June 19, 1992 (“FADP”) or by any subsequent act, including the relevant amendments and implementing ordinances (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established).
 - iii.** The data importer acknowledges and agrees that the personal data transferred to data importer by data exporter may include personal data of legal persons and personality profiles of natural persons. The data importer shall process personal data of legal persons in the same manner as other personal data and personality profiles in the same manner as special categories of data (the special protection of data from legal persons and from personality profiles will be abolished upon entering into force of the revised Swiss Federal Data Protection Act of September 25, 2020 (“R-FADP”)).
 - iv.** “Member State” shall be interpreted as including Switzerland.
 - v.** The term “Member State” must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their habitual place of residence (Switzerland) in accordance with Clause 18c. June 19, 1992 (“FADP”) or by any subsequent act, including the relevant amendments and implementing ordinances (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established).

In the event Client transfers Client Personal Data that relates to data subjects in Switzerland to Maverick, this Section 15.b. shall modify the corresponding references in this DPA. For clarity and avoidance of doubt, this Section 15.b. will amend this DPA to

the extent necessary for compliance with the Swiss Federal Act on Data Protection. This Section 15.b. shall only apply to personal data subject to the Swiss Federal Act on Data Protection.

- c. In respect of any Restricted Transfer subject to the UK GDPR, the Parties hereby enter into the UK IDTA (with Client as data exporter and Maverick as data importer), which is incorporated by reference into this DPA and which shall come into effect upon the commencement of a Restricted Transfer. The Parties make the following selections for the purpose of the UK IDTA:

Part 1: Tables

- i. Table 1
 1. The Start Date is the Effective Date of the Agreement.
 2. The Exporter is the Client and the Importer is Maverick.
 3. The Exporter's details are found in the Agreement. The Importer is Maverick Training Corporation DBA Maverick Solutions, a North Carolina corporation, with principal address at 3150 Rogers Road, Suite 200, Wake Forest, North Carolina, 27587, USA.
 4. The Exporter's Key Contact is found in the Agreement. The Importer's Key Contact is the Security and Compliance Manager, who can be reached at security@mavericksolutions.net.
- ii. Table 2: The Parties choose the EEA SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the EEA SCCs brought into effect for the purposes of this IDTA:
 1. Clause 7 – See Section 15.a.i. above.
 2. Clause 9 – See Section 15.a.ii above.
 3. Clause 11 – See Section 15.a.iii above.
- iii. Table 3
 1. Annex 1A: See Appendix 1.
 2. Annex 1B: See Appendix 1.
 3. Annex II: See Appendix 2.
 4. Annex III: N/A.
- iv. Table 4
 1. The Importer may end this IDTA.

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.

- d. In respect of any relevant transfer between Maverick and a Sub-Processor, Maverick shall either enter into Module Three of the EEA SCCs or Module Three of the EEA SCCs as modified by the UK IDTA, where doing so is necessary to ensure that the relevant transfer complies with Applicable Data Protection Laws.

- e. For the avoidance of doubt, if, and to the extent that, the European Commission or the UK Government issues any amendment to, or replacement of, the EEA SCCs or UK IDTA pursuant to Article 46(5) GDPR or Article 46 of the UK GDPR, the parties acknowledge and agree that such clauses will automatically be deemed to replace all Standard Contractual Clauses then in force between the Client and Maverick and the parties shall take such additional steps as necessary to give ensure that such replacement terms are implemented across all transfers.
- f. If, at any time, a supervisory authority or a court with competent jurisdiction over a party mandates that certain cross-border transfers from Controllers to Processors must be subject to specific additional safeguards (including but not limited to specific technical and organizational measures), the parties shall work together in good faith to implement such safeguards and ensure that any transfer of Client Personal Data is conducted with the benefit of such additional safeguards.

Appendix 1

Description of Data Processing

1. Subject matter and duration of the Processing of Client Personal Data

The subject matter and duration of the Processing of the Personal Data are set out in the Agreement and this DPA.

2. The nature and purpose of the Processing of Client Personal Data

Maverick is engaged to provide Services to Client which involve the Processing of Personal Data. The Client Personal Data shall be processed in order to provide the Service to Customer, including:

- the performance of the Agreement;
- technical support;
- compliance with data exporter requests;
- communication of directions by data exporter; and
- service updates.

3. The types of the Personal Data to be Processed

- Employees of the Client
 - First and Last Name (optionally provided by data subject)
 - Professional Email address
 - Professional Username/User ID
 - Job role
 - Time zone

4. The categories of Data Subject to whom the Personal Data relates

The Data Subjects are the employees of the Client.

5. The obligations and rights of Client

The obligations and rights of Client are set out in the Agreement and this DPA.

6. Frequency of restricted transfers (where applicable)

As necessary to deliver Services for the duration of the Agreement.

7. The period for which Client Personal Data subject to restricted transfers will be retained (where applicable)

In accordance with the Client's instructions (and otherwise for the duration of the Agreement), except where Maverick retains Client Personal Data to comply with applicable laws or to establish, exercise or defend legal rights, in accordance with its data retention policies.

Appendix 2

Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

Maverick uses the following technical and organization measures as part of its security program designed to protect the security of Client Personal Data:

- TLS 1.2 and 1.3 encryption of data in transit
- AES-256 encryption of data at all points of rest
- Principles of least privilege and separation of duties for all staff
- Internal data privacy and data protection training done annually
- Authenticated and unauthenticated penetration testing of the applicable services
- Static Application Security Testing and Dynamic Application Security Testing Vulnerability Scanning of the applicable services
- Strict adherence to data minimization principles to collect and store as little data as is possible to provide services
- Salting and hashing off all credential data within encrypted storage end-points
- Measures to allow for all GDPR defined data subject request rights
- Data sanitization processes and procedures

Appendix 3

List of Sub-Processors

The Client has authorized the use of the following sub-processors:

| Apty | |
|--|--|
| Address | Contact |
| 1524 S I-35 Frontage Road Suite 224 Austin, TX 78704 USA | Shafiq Walji Director of Customer Success <contact info can be given upon request> |
| Description of Processing | |
| Apty creates and maintains the underlying software capabilities that are leveraged by our Engage Live offering. Apty also collects and stores the data that is created by the use of Engage Live; this data is under our explicit control at all times and is hosted on AWS servers. | |

| AWS | |
|--|---|
| Address | Contact |
| Virginia USA | No direct contact person, we have access to staff via a portal. |
| Description of Processing | |
| AWS is the IaaS for our SaaS. It hosts our DB as well as the PaaS and can be assumed to touch all application associated data. | |

| Azure | |
|---|---|
| Address | Contact |
| Virginia USA | No direct contact person, we have access to staff via a portal. |
| Description of Processing | |
| Azure is currently being used to store content related to the learning paths in our application. No PII is stored here. It is called upon using pull requests initiated by the Dyno servers (AWS IaaS) of Heroku. | |

| Heroku | |
|---|---|
| Address | Contact |
| 415 Mission Street Suite 300 San Francisco, CA 94105 USA | No direct contact person, we have access to staff via a portal. |

| Description of Processing |
|--|
| The PaaS for our SaaS who is also responsible for the setup and maintenance of our IaaS. They allow us to focus on deploying, managing, and scaling the elements of our SaaS that are SaaS specific with a simplified UI and integration tooling to allow for easier platform and infrastructure management. Heroku also hosts our relational DB in which our tenants and their associated data are stored, we have full interactive control of this DB. More in depth information and documentation can be found at https://devcenter.heroku.com . |

| Microsoft SharePoint | |
|---|---|
| Address | Contact |
| One Microsoft Way Redmond, Washington 98052-6399 USA | No direct contact person, we have access to staff via a portal. |
| Description of Processing | |
| SharePoint is leveraged by Maverick Solutions as a data storage location. Files uploaded to Monday.com will be accessed via SharePoint by Maverick personnel as well as client personnel. More information can be found here: https://learn.microsoft.com/en-us/sharepoint/ | |

| Monday.com | |
|--|---|
| Address | Contact |
| 225 Park Avenue South New York, NY 10003 USA | No direct contact person, we have access to staff via a portal. |
| Description of Processing | |
| Monday is a project and task tracking tool that is used by Maverick to keep track of the imported data from customers as well as liase it to our storage point, it will also be used by customers to directly import the data. More information can be found here: https://developer.monday.com/apps/docs | |

| SendGrid | |
|--|---|
| Address | Contact |
| 1801 California Street Suite 500 Denver, CO 80202 USA | No direct contact person, we have access to staff via a portal. |
| Description of Processing | |
| SendGrid is a cloud-based SMTP which we leverage to send out our account management emails (primarily onboarding emails that notify a user that they have access to Engage Learn). | |

Effective: April 1, 2025