

PRIVACYTEAM CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) is incorporated by reference into PrivacyTeam’s Terms of Service (available at <https://protected.fm/lp-term-conditions/>) or other agreement governing the provision of the Services (as defined below) (“**Agreement**”) entered by and between you, the Customer (“**Customer**”, as defined in the Agreement), and Privacy Team Ltd. (“**PrivacyTeam**”) to reflect the parties’ agreement with regard to the Processing of Personal Data by PrivacyTeam on behalf of the Customer when providing the Services. Both parties shall be referred to as the “**Parties**” and each, a “**Party**”.

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement. In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail.

Definitions

“**CCPA**” means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq.

“**Data Protection Laws**” means all binding privacy and data protection laws and regulations, including (without limitation) the GDPR, the UK GDPR, the FADP, the CCPA and Israel’s Protection of Privacy Law 5741-1981, each to the extent applicable to the Processing of Personal Data hereunder and in effect at the time of Processor’s performance hereunder.

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

“**FADP**” means the Swiss Federal Act on Data Protection of 19 June 1992, and as revised as of 25 September 2020, the “Revised FADP”.

“**GDPR**” means the General Data Protection Regulation (EU) 2016/679.

“**Personal Data**” means any information relating to an identified or identifiable natural person which is processed by PrivacyTeam on Customer’s behalf under the Agreement and this DPA.

“**Services**” means PrivacyTeam’s Privacy Training Services as further detailed in the Agreement.

“**Standard Contractual Clauses**” shall mean (i) where the GDPR applies, Module 2 of the standard clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (“EU SCCs”); or (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner’s Office in the UK of 21 March 2022 (“UK SCCs”).

“**Sub-processor**” means a third party that Processes Personal Data on behalf, and under the instruction, of PrivacyTeam.

“**UK GDPR**” means the GDPR as it forms part of the law of the United Kingdom.

The terms, “**Controller**”, “**Member State**”, “**Processor**”, “**Processing**” and “**Supervisory Authority**” shall have the same meaning as in the GDPR.

For the purpose of clarity, to the extent that the CCPA applies, the terms “**Controller**” shall also mean “**Business**”, and “**Processor**” (including “**Sub-processor**”) shall also mean “**Service Provider**”.

1. **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data (i) Customer is the Controller of the Personal Data, (ii) PrivacyTeam is the Processor of the Personal Data.
2. **Customer’s Processing of Personal Data.** Customer, in its use of the Services, and Customer’s instructions to PrivacyTeam, shall comply with Data Protection Laws. Customer shall establish and have any and all required legal bases in order to collect, Process and transfer to PrivacyTeam the Personal Data, and to authorize the Processing by PrivacyTeam on Customer’s behalf in accordance with the Agreement.
3. **PrivacyTeam’s Processing of Personal Data.** PrivacyTeam shall Process Personal Data for the following purposes: (i) Processing to provide the Services in accordance with the Agreement and this DPA; (ii) Processing to comply with Customer’s reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement; (iii) rendering Personal Data non-identifiable and anonymous; (iv) Processing as required under applicable laws, provided that PrivacyTeam shall

inform Customer of the legal requirement before Processing, unless such law or order prohibit disclosing such information. PrivacyTeam shall inform Customer without undue delay if, in PrivacyTeam's opinion, the instructions for the Processing of Personal Data given by Customer infringes Data Protection Laws.

4. **CCPA Standard of Care; No Sale of Personal Information.** PrivacyTeam acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that PrivacyTeam provides to Customer under the Agreement. PrivacyTeam shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Customer's behalf, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as stipulated in the Agreement and this DPA. PrivacyTeam certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Personal Information Processed hereunder without Customer's prior written consent, nor taking any action that would cause any transfer of Personal Information to or from PrivacyTeam under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA.
5. **Details of the Processing.** The subject matter, duration, nature and purpose of the Processing, as well as the types of Personal Data Processed under this DPA and the categories of Data Subjects concerned are further specified in Schedule 1 (Details of Processing) to this DPA.
6. **Data Subject Requests.** If a request from Data Subjects to exercise their rights under Data Protection Laws ("Data Subject Request(s)") has been received by PrivacyTeam, PrivacyTeam shall either (i) notify Customer of such request, or (ii) refer the Data Subject to Customer. Taking into account the nature of the Processing, PrivacyTeam shall reasonably assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws.
7. **Confidentiality.** PrivacyTeam shall ensure that its personnel and advisors engaged in the Processing of Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
8. **Sub-Processors.** Customer acknowledges and agrees that PrivacyTeam engages with Sub-processors to provide the Services and Customer hereby authorizes the use of the Sub-processors currently used. PrivacyTeam may appoint new Sub-processors (or replace existing ones) in which case it will give notice of the planned appointment to Customer and Customer may reasonably object to the use of the new Sub-processor in writing within seven (7) days following receipt of such notice. If no such objection is provided within that time, the appointment of such new Sub-processor shall be deemed authorized by Customer. In the event Customer reasonably objects as per the above, PrivacyTeam will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor. If PrivacyTeam is unable to make available such change within 30 days following receipt of Customer's objection, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA.

PrivacyTeam has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data and containing the same, or materially similar, data protection obligations as set out in this DPA. Where the Sub-processor fails to fulfill its data protection obligations, PrivacyTeam shall remain liable to the Customer for the performance of the Sub-processor's obligations.

9. **Controls for the Protection of Personal Data.** PrivacyTeam shall maintain industry-standard technical and organizational measures for the protection of Personal Data Processed hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data, confidentiality and integrity of Personal Data), 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. Upon the Customer's written request, PrivacyTeam will reasonably assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the Processing and the information available to PrivacyTeam.
10. **Audits and Inspections.** Upon Customer's 14 days prior written request at reasonable intervals (no more than once every 12 months), and subject to strict confidentiality undertakings by Customer, PrivacyTeam shall make available to Customer (or Customer's independent, reputable, third-party auditor that is not a

competitor of PrivacyTeam and not in conflict with PrivacyTeam, subject to strict confidentiality and non-compete undertakings) information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without PrivacyTeam's prior written approval). Upon PrivacyTeam's first request, Customer shall return all records or documentation in Customer's possession or control provided by PrivacyTeam in the context of the audit and/or the inspection. In the event of an audit or inspections as set forth above, Customer shall ensure that it (or each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to PrivacyTeam's premises, equipment, personnel and business while conducting such audit or inspection.

- 11. Data Incident Management and Notification.** PrivacyTeam shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data ("**Data Incident**"). PrivacyTeam shall make reasonable efforts to identify and take those steps as PrivacyTeam deems necessary and reasonable in order to remediate and/or mitigate the cause of a Data Incident to the extent the remediation and/or mitigation is within PrivacyTeam's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or anyone who uses the Services on Customer's behalf.
- 12. Return And Deletion of Personal Data.** Within 30 days following termination of the Agreement and subject thereto, PrivacyTeam shall, at the choice of Customer (indicated in written notification), delete or return to Customer all the Personal Data unless applicable laws require otherwise.
- 13. Cross-Border Data Transfers.**
 - 12.1. Transfers from the EEA, the United Kingdom and Switzerland to countries that offer adequate level of data protection.** Personal Data may be transferred from the European Economic Area ("**EEA**"), Switzerland and the United Kingdom ("**UK**") to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant authorities ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary.
 - 12.2. Transfers from the EEA, the United Kingdom and Switzerland to other countries.** If the Processing of Personal Data by PrivacyTeam includes a transfer (either directly or via onward transfer) from the EEA ("**EEA Transfer**"), the UK ("**UK Transfer**"), and/or Switzerland ("**Swiss Transfer**") to countries that are not subject to an Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by PrivacyTeam for the lawful transfer of personal data (as defined in the GDPR, the UK GDPR, the FADP, as relevant) outside the EEA, the UK or Switzerland, as applicable, then (i) the terms set forth in Part 1 of Schedule 2 (EEA Cross Border Transfers) shall apply to EEA Transfers; (ii) the terms set forth in part 2 of Schedule 2 (UK Cross Border Transfers) shall apply to UK Transfers, and (iii) the terms set forth in Part 3 of Schedule 2 (Swiss Cross Border Transfers) shall apply to Swiss Transfers.
- 14. Data Protection Impact Assessment and Prior Consultation.** Upon Customer's reasonable request, PrivacyTeam shall provide Customer, at Customer's cost, reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR or the UK GDPR (to the extent applicable) to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to PrivacyTeam. PrivacyTeam shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks, to the extent required under the GDPR or the UK GDPR.
- 15. Modifications.** Each Party may by at least forty-five (45) calendar days' prior written notice to the other Party, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of Customer Personal Data to be made (or continue to be made) without breach of those Data Protection Laws. The Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's or PrivacyTeam's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days of such notice, then Customer or PrivacyTeam may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof).

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Services;
2. Performing the Agreement and this DPA;
3. Complying with applicable laws and regulations;
4. All tasks related with any of the above.

Duration of Processing

Subject to the DPA and/or the Agreement, PrivacyTeam will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

- User's name, organizational email, position, workplace, and any other information submitted by the user or the Customer for the purpose of user registration and login;
- User's training progress, quiz answers and scoring.

Categories of Data Subjects

- Users of the Services who are Customer's employees or are otherwise directed by Customer to use the Services on Customer's behalf.

SCHEDULE 2 – CROSS BORDER TRANSFERS

Part 1 – EEA Transfers

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to an EEA Transfer.
2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and PrivacyTeam is the data processor of the Personal Data.
3. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.
4. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the Standard Contractual Clauses shall apply, and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 8 of the DPA.
5. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.
6. In Clause 17 of the Standard Contractual Clauses, Option 1 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland.
7. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of the Republic of Ireland.
8. Annex I.A of the Standard Contractual Clauses shall be completed as follows:
 - Data Exporter: Customer.
 - Contact details: As detailed in the Agreement.
 - Data Exporter Role: The Data Exporter is a data controller.
 - Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
 - Data Importer: PrivacyTeam.
 - Contact details: As detailed in the Agreement.
 - Data Importer Role: The Data Importer is a data processor.
 - Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
9. Annex I.B of the Standard Contractual Clauses shall be completed as follows:
 - The categories of data subjects are described in Schedule 1 (Details of Processing) of this DPA.
 - The categories of personal data are described in Schedule 1 (Details of Processing) of this DPA.
 - The frequency of the transfer is a continuous basis for the duration of the Agreement.
 - The nature of the processing is described in Schedule 1 (Details of Processing) of this DPA.
 - The purpose of the processing is described in Schedule 1 (Details of Processing) of this DPA.
 - The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.
 - In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth at the link detailed in Section 8 of the DPA.
10. Annex I.C of the Standard Contractual Clauses shall be completed as follows: The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 7 above.
11. The Security Documentation referred to in the DPA serves as Annex II of the Standard Contractual Clauses.
12. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.

Part 2 – UK Transfers

The parties agree that the terms of the UK SCCs (i.e. the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner's Office in the UK) are hereby incorporated by reference and shall apply to UK Transfers. The relevant tables in the UK SCCs shall be deemed completed with the details set forth in Schedule 1 and Schedule 2 of this DPA as appropriate.

Part 3 – Swiss Cross Border Transfers

The Parties agree that the Standard Contractual Clauses as detailed in Part 1 of this Schedule 2, shall be adjusted as set out below where the FADP applies to Swiss Transfers:

1. References to the Standard Contractual Clauses mean the Standard Contractual Clauses as amended by this Part 3;
2. The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss Transfers exclusively subject to the FADP;
3. The terms “General Data Protection Regulation” or “Regulation (EU) 2016/679” as utilized in the Standard Contractual Clauses shall be interpreted to include the FADP with respect to Swiss Transfers;
4. References to Regulation (EU) 2018/1725 are removed;
5. Swiss Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in Part 1 of this Schedule 2;
6. References to the “Union”, “EU” and “EU Member State” shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses;
7. Where Swiss Transfers are exclusively subject to the FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP;
8. Where Swiss Transfers are subject to both the FADP and the GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP insofar as the Swiss Transfers are subject to the FADP;
9. The Standard Contractual Clauses as amended by this Part 3 also protect the Personal Data of legal entities until the entry into force of the Revised FADP.