Data Processing Addendum

Last Updated June 30, 2021

This Data Processing Addendum (together with its Annexes, this "DPA") forms part of the Agreement, as defined in the Entaice LLC Terms of Service, and is made between Entaice LLC (the "Entaice") and Entaice's customers (each, a "Customer") and, with respect to each Customer, shall be effective as of the date that such Customer enters into the Agreement with Entaice. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In the course of providing the Service to Customer pursuant to the Agreement, Entaice may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any such Personal Data.

1. **Definitions.** Unless otherwise set out below, each capitalized term in this DPA shall have the meaning set out in the Agreement, and the following capitalized terms used in this DPA shall be defined as follows:
   1.1. "Customer Personal Data" means the "personal data" (as defined in the Standard Contractual Clauses) and any other personal data that Entaice processes on behalf of Customer or Customer's affiliate in connection with Entaice's provision of the Service.
   1.2. "Data Protection Laws" means all laws and regulations applicable to the processing of Personal Data, including (a) the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council (the "GDPR"), any national implementing or supplementary legislation and any other applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of Customer Personal Data, and (b) the California Consumer Privacy Act of 2018 (the "CCPA"), including any regulations promulgated thereunder, as amended from time to time.
   1.3. "European Economic Area" or "EEA" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein.
   1.4. "Personal Data" shall mean any information that (a) identifies or relates, directly or indirectly, to a natural person, or (b) the relevant Data Protection Law otherwise defines as personal data or a similar term.
   1.5. "Security Incident" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Personal Data.
   1.6. "Standard Contractual Clauses" means the Standard Contractual Clauses (processors) approved by European Commission Decision C(2010)593 set out in Annex 1 to this DPA or any subsequent version thereof released by the European Commission (which will automatically apply), and which includes Annex 2 (Details of the Processing and Transfer) and Annex 3 (Technical and Organizational Measures) to this DPA.
   1.7. "Subprocessor" means any Processor engaged by Entaice who agrees to receive from Entaice Customer Personal Data.
   1.8. "US" means the United States of America.
   1.9. The terms "Controller", "Processor", "Data Subject", "Process" and "Supervisory Authority" shall have the same meaning as set out in the GDPR.
   1.10. The terms "service provider", and "sell" (and "selling", "sale", and "sold") shall have the same meaning as set out in the CCPA.
2. **Processing of Personal Data**
   2.1. *Instructions for Data Processing*. Entaice will only Process, retain, use, or disclose Customer Personal Data as a Processor, or service provider, in accordance with the Agreement, to the extent necessary to provide the Service to the Customer, and the Customer's written instructions (the "Permitted Purpose"), unless Processing is required by the Data Protection Laws to which Entaice is subject, in which case Entaice shall, to the extent permitted by the Data Protection Laws, inform the Customer of that legal requirement before Processing that Customer Personal Data. Entaice shall not sell Customer Personal Data, nor Process, retain, use, or disclose Customer Personal Data (a) for any purposes other than the Permitted Purpose, or (b) outside of the direct business relationship between Entaice and Customer. Entaice certifies that it understands these restrictions and will comply with them. The Agreement (subject to any

changes to the Service agreed between the parties) and this DPA shall be the Customer's complete and final instructions to Entaice in relation to the processing of Customer Personal Data. Processing outside the scope of this DPA or the Agreement will require prior written agreement between the Customer and Entaice on additional instructions for Processing.

2.2. *Required consents.* The Customer shall provide all applicable notices to Data Subjects required under applicable Data Protection Laws for the lawful Processing of Customer Personal Data by Entaice in accordance with the Agreement. Where required by applicable Data Protection Laws, Customer will ensure that it has obtained/will obtain all necessary consents for the lawful Processing of Customer Personal Data by Entaice in accordance with the Agreement.

3. Transfer of Personal Data

3.1. *Authorized Subprocessors.* The Customer agrees that Entaice may use Subprocessors, including Amazon Web Services, Google Cloud Platform and Microsoft Azure, to Process Customer Personal Data, provided it enters into a written agreement with the Subprocessor which imposes the substantially similar obligations on the Subprocessor with regard to their Processing of Customer Personal Data as are imposed on Entaice under this DPA.

3.2. *Changes to Subprocessors.* Entaice shall notify the Customer from time to time of the identity of any Subprocessors it engages. If the Customer (acting reasonably) does not approve of a new Subprocessor, then without prejudice to any right to terminate the Agreement, the Customer may request that Entaice moves the Customer Personal Data to another Subprocessor and Entaice shall, within a reasonable time following receipt of such request, use all reasonable efforts to ensure that the Subprocessor does not Process any of the Customer Personal Data. If it is not reasonably possible to use another Subprocessor, and Customer continues to object for a legitimate reason, either Party may terminate the Agreement on thirty (30) days written notice. If the Customer does not object within thirty (30) days of receipt of the notice, the Customer is deemed to have accepted the new Subprocessor.

3.3. *Liability of Subprocessors.* Entaice shall at all times remain responsible for compliance with its obligations under this DPA and will be liable to the Customer for the acts and omissions of any Subprocessor approved by the Customer as if they were the acts and omissions of Entaice.

3.4. *Prohibition on Transfers of Personal Data.* To the extent that the Processing of Customer Personal Data by Entaice involves the export of such Customer Personal Data to a country or territory outside the EEA, other than to a country or territory ensuring an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of personal data as determined by the European Commission (an "International Transfer"), such transfer shall be governed by the Standard Contractual Clauses. In the event of any conflict between any terms in the Standard Contractual Clauses, this DPA and the Agreement, the Standard Contractual Clauses shall prevail.

4. Data Security; Audits; Security Notifications

4.1. *Entaice Security Obligations.* 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, Entaice shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures set out in Annex 3.

4.2. Upon request by the Customer, Entaice shall make available all information reasonably necessary to demonstrate compliance with this DPA.

4.3. *Security Incident Notification.* If Entaice or any Subprocessor becomes aware of a Security Incident, Entaice will (a) notify the Customer of the Security Incident within seventy-two (72) hours, (b) investigate the Security Incident and provide such reasonable assistance to the Customer (and any law enforcement or regulatory official) as required to investigate the Security Incident, and (c) take steps to remedy any noncompliance with this DPA.

4.4. *Entaice Employees and Personnel.* Entaice shall treat the Customer Personal Data as the confidential information of the Customer, and shall ensure that any employees or other personnel have agreed in writing to protect the confidentiality and security of Customer Personal Data.

5. Access Requests; Data Subject Rights

5.1. *Data Subject Requests*. Except as required (or where prohibited) under applicable law, Entaice shall notify Customer of any request received by Entaice or any Subprocessor from a Data Subject in respect of their Personal Data included in the Customer Personal Data and shall not respond to the Data Subject.

5.2. Entaice shall provide Customer with the ability to correct, delete, block, access or copy the Customer Personal Data in accordance with the functionality of the Service.

5.3. *Government Disclosure*. Entaice shall notify Customer of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency.

5.4. *Data Subject Rights*. Where applicable, and taking into account the nature of the Processing, Entaice shall use all reasonable efforts to assist Customer by implementing any other appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising Data Subject set forth in the GDPR.

5.5. *Audits*. Entaice will, upon reasonable request from the Customer, allow for and contribute to audits, including inspections, conducted by the Customer (or a third party auditor on behalf of, and mandated by, the Customer) provided (a) such audits or inspections are not conducted more than once per year (unless requested by a Supervisory Authority); (b) are conducted only during business hours; and (c) are conducted to cause minimal disruption to Entaice's operations and business. The Customer shall reimburse Entaice any fees or costs incurred by Entaice in conducting (or arranging the conduct of) any audits in accordance with this Section 5.5.

6. Data Protection Impact Assessment; Prior Consultation

6.1. To the extent required under applicable Data Protection Laws, Entaice shall provide reasonable assistance to the Customer with any data protection impact assessments and with any prior consultations to any Supervisory Authority of Customer, in each case solely in relation to Processing of Customer Personal Data and taking into account the nature of the Processing and information available to Entaice.

7. Termination

7.1. *Deletion of data*. Subject to Section 7.2 below, Entaice shall, within ninety (90) days of the date of termination of the Agreement, delete and use all reasonable efforts to procure the deletion of all other copies of Customer Personal Data Processed by Entaice or any Subprocessors.

7.2. Entaice and its Subprocessors may retain Customer Personal Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws and always provided that Entaice shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

8. Notification of Potential Applicability of US Surveillance Laws/Orders

8.1. Entaice is a US company headquartered in the US. As such, Entaice is generally subject to US laws, including laws which may impact Entaice's obligations pursuant to this DPA and the Standard Contractual Clauses. In accordance with those obligations, Entaice hereby notifies the Customer of the following: (a) like many US-based data processors, Entaice may be subject to Section 702 of the US Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a ("FISA Section 702"), and therefore may be eligible to receive upstream or bulk surveillance orders under FISA Section 702; and (b) Executive Order 12333 ("EO 12333") does not provide the US government the ability to order or demand Entaice to provide assistance for the bulk collection of information and Entaice will not do so voluntarily. Entaice shall encrypt all transfers of Customer Personal Data, which can prevent the acquisition of such data by US governmental authorities pursuant to EO 12333, while that data is in transit. As of the date of this DPA, Entaice has not received any requests under FISA Section 702 or EO 12333.

ANNEX 1 TO DATA PROCESSING ADDENDUM: STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of this Annex 1, references to the "data exporter" and "data importer" shall be to the Customer and to Entaice respectively (each a " party "; together " the parties ").

Clause 1

Definitions

For the purposes of the Clauses:

(a) '*personal data*', *'special categories of data'*, *'process/processing'*, *'controller'*, *'processor'*, *'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the Transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in ANNEX 2 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in ANNEX 3 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of ANNEX 3, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Annex 3 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:
   (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
   (ii) any accidental or unauthorised access, and
   (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of ANNEX 3 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

ANNEX 2 TO DATA PROCESSING ADDENDUM: DETAILS OF THE PROCESSING AND TRANSFER OF CUSTOMER PERSONAL DATA

Data exporter: Customer

Data importer: Entaice

Data subjects: Authorized users and any other data subjects whose data the Customer or its authorized users provide via the Service.

Categories of data: Contact information, usage information, nontraditional identifiers of the Customer's authorized users, and any other Personal Data the Customer or its authorized users submit to the Service.

Processing operations: The Processing of Customer Personal Data provided by the Customer to Entaice through the Platform or otherwise in connection with the provision of the Service.

Subject matter and duration of the Processing of Customer Personal Data: The subject matter and duration of the processing are as set out in the Agreement and this DPA.

The nature and purpose of the Processing of Customer Personal Data: The Processing of Customer Personal Data provided by the Customer to Entaice through the Service or otherwise in connection with the provision of the Service.

The obligations and rights of the Customer: The obligations and rights of the Customer are as set out in this DPA.

ANNEX 3 TO DATA PROCESSING ADDENDUM: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

1. Entaice maintains internal policies and procedures, or procures that its Subprocessors do so, which are designed to:

    a. secure any personal data Processed by Entaice against accidental or unlawful loss, access or disclosure;

    b. identify reasonably foreseeable and internal risks to security and unauthorized access to the personal data Processed by Entaice; and

    c. minimize security risks, including through risk assessment and regular testing.

2. Entaice will, and will use reasonable efforts to procure that its Subprocessors conduct periodic reviews of the security of their network and the adequacy of their information security program as measured against industry security standards and its policies and procedures.

3. Entaice will, and will use reasonable efforts to procure that its Subprocessors periodically evaluate the security of their network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.